KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **PW0-204**

Title : Certified Wireless Security Professional (CWSP)

Version : DEMO

1.In an effort to optimize WLAN performance ABC Company has already upgraded their infrastructure from 802 11b/g to 802 11n. ABC has always been highly security conscious but they are concerned with security threats introduced by incompatibilities between 802.11n and 802.11a/g in the past. ABC has performed manual and automated scans with products that were originally designed for use in 802 11a/g networks. Including laptop-based spectrum and protocol analyzers as well as an overlay 802 11a/g WIPS solution. ABC has sought your input to understand and respond to potential security threats.
In ABC's network environment, what type of devices would be capable of identifying rouge APs that use HT Greenfield 40 MHZ channels? (Choose 3)
A. 802.11n WPS sensor with a single 2x2 radio
B. The company's current laptop-based protocol analysis tools
C. WIPS solution that is integrated in the company's AP infrastructure
D. The company's current overlay WIPS solution
E. The company's current laptop-based spectrum analysis tools
Answer: A,B,C
Explanation: HT GreenfieldThe Greenfield PHY header is not backward compatible with legacy 802.11a/g radios and can only be interpreted by 802.11n HT radios
0470438916.pdf,Page 410
Laptop Analyzer automatically identifies hundreds of performance problems, such as 11b/g conflicts, 802.11e problems, and QoS, as well as dozens of wireless intrusions and hacking strategies, including Rogue devices. With the Laptop Analyzer, users can classify and decode Non-HT (legacy), HT mixed format and HT greenfield format traffic and identify backward compatibility issues with legacy 802.11a/b/g devices operating in the same environment.
http://www.njbo.net/tools/Laptop%20Analyzer%20%20WLAN%20Monitoring%20and%20Troubleshooting%20Tool%20-%20AirMagnet.htm
The HT Greenfi eld PHY header cannot be detected by a WIPS that is using legacy 802.11a/g sensors. The solution to this problem is to upgrade the WIPS with new sensors that also have 802.11n HT radios. (the company has already upgraded to 802.11n so C is correct)

2.Given: A new Access point is connected to an authorized network segment and is detected wirelessly by a WIPS.
By what method does the WIPS apply a security classification to newly discovered AP?
A. According to the location service profile
B. According to the SNMP MIB table
C. According to the RADIUS rectum attribute
D. According to the site survey template
E. According to the default security policy
Answer: B
Explanation: http://webcache.googleusercontent.com/search?q=cache:Exehyw9ijwJ:www.nhbook.com/exam/PW0200.pdf+A+new+Access+point+is+connected+to+an+authorized+network+segment+and+is+detec ted+wirelessly+by+a+WIPS.+WIPS+uses+location+service+profile&cd=9&hl=en&ct=clnk&gl=in&source=www.google.co.in

3.What elements should be addressed by a WLAN security policy? (Choose 2)
A. Verification that administrative passwords are unique to each infrastructure device

B. Enabling encryption to prevent MAC addresses from being sent in clear text
C. Security policy details should be safeguarded from non IT employees to prevent vulnerability exposure
D. End user training for password selection and acceptable network use
E. Social engineering recognition and mitigation technique.
Answer: D,E
Explanation:
A proper password security policy for wireless access should be ensured, and the baseline for secure password and secret key selection should be enforced.
As part of a more general corporate security policy, users should be informed about social engineering attacks and not disclosing information about the network to potential attackers.
http://e-articles.info/e/a/title/Wireless-Security-Policy/

4.Role-based access control (RBAC) allows a WLAN administrator to perform that network function?
A. Allows access to specific files and applications based on the user's WMM AC.
B. Provide admission control to VoWiFi clients on selected access points.
C. Allows one user group to access an internet gateway while denying internet access gateway to another group
D. Provide differing levels of management access to a WLAN controller based on the user account.
E. Allow simultaneous support of multiple EAP types on a single Access point.
Answer: D
Explanation: http://dnscoinc.com/bradfordidentity.pdf

5.The following numbered items show the contents of the four frames exchanged during the 4-way handshake.
-Encrypted GTK sent -Confirmation of temporal key installation -Announce sent from authenticator to supplicant, unprotected by MIC -Snonce sent from applicant to authenticator, protected by MIC.
Arrange the frames in the correct sequence beginning with the start of the 4-way handshake
A. 3, 4, 1, 2
B. 2, 3, 4, 1
C. 1, 2, 3, 4
D. 4, 3, 1, 2
Answer: A

6.What 802 11 WLAN security problem is addressed by 802.1X/EAP mutual authentication.
A. Disassociation attacks
B. Weak initialization vectors
C. Offline dictionary attacks
D. Weak password policies
E. MAC spoofing
F. Wireless hijacking attacks
Answer: F
Explanation: The only way to prevent a wireless hijacking, man-in-the-middle, and/or Wi-Fi phishing attack is to use a mutual authentication solution.802.1X/EAP authentication solutions require that mutual authentication credentials be exchanged before a user can be authorized.

7.What disadvantage does EAP-TLS have when compared with PEAPvO EAP/MSCHAPv2 as an 802. 11 WLAN security solution?

A. EAP-TLS requires a PKI to create X509 certificates for both the server and client, which increases administrative overhead.

B. EAP-TLS does not use SSL to establish a secure tunnel for internal EAP authentication.

C. Fast/secure roaming in an 802 11 RSN is significantly longer when EAP-TLS is use.

D. EAP-TLS does not protect the client's username and password in side an encrypted tunnel.

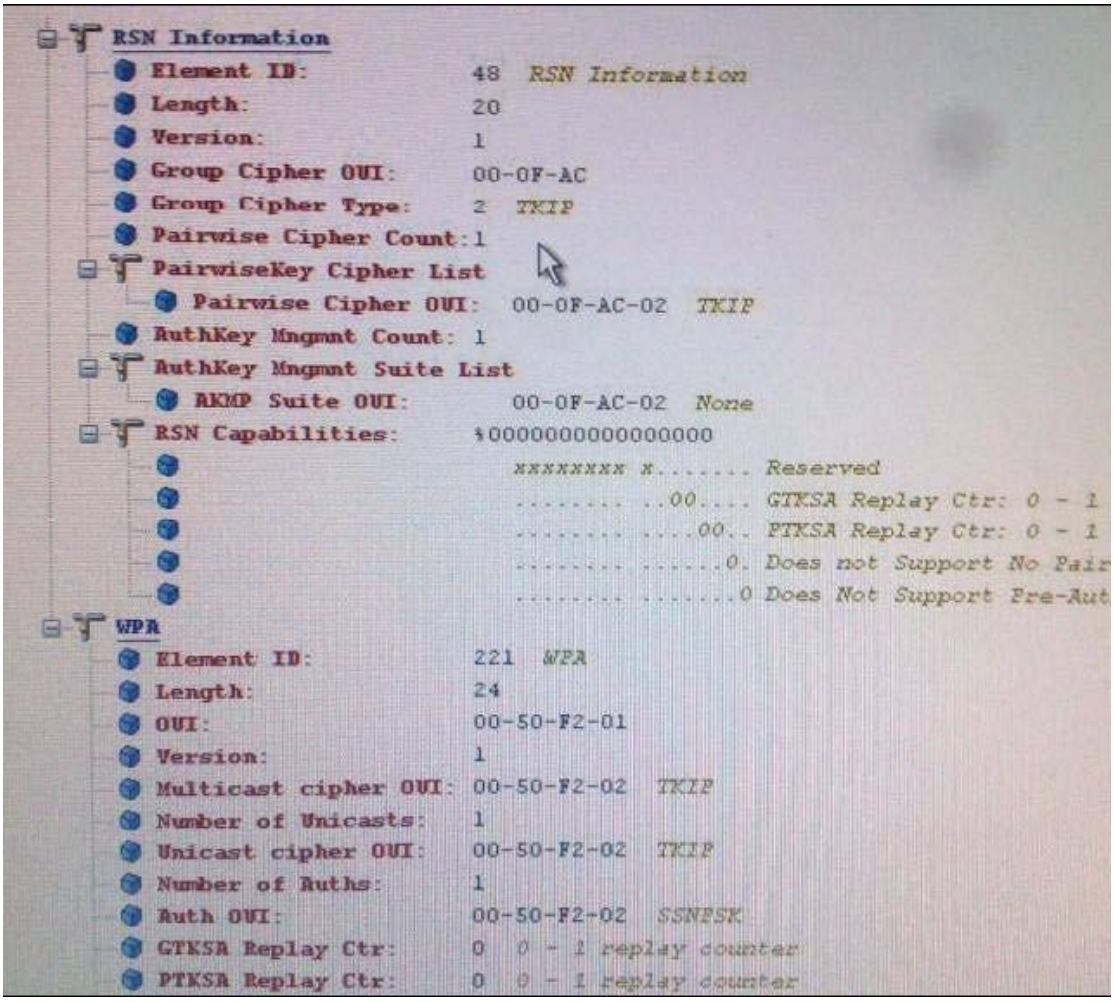
E. Though more secure EAP-TLS is not widely supported by wireless infrastructure or client vendors.

F. Initially mobility authentication with EAP-TLS is significantly longer due to X509 certificate verification.

Answer: A

Explanation: EAP - TLS requires the use of client - side certifi cates in addition to a server certifi cate.The biggest factor when deciding to implement EAP - TLS is whether an enterprise PKI infrastructure is already in place. This would usually, and optimally, include separate servers in a high - availability server cluster.

8.Exhibit Given: The illustration shows a WLAN protocol analyzer decoding an 802.11 beacon frame.



What statement about the access points BSS is true and can be confirmed with this illustration?

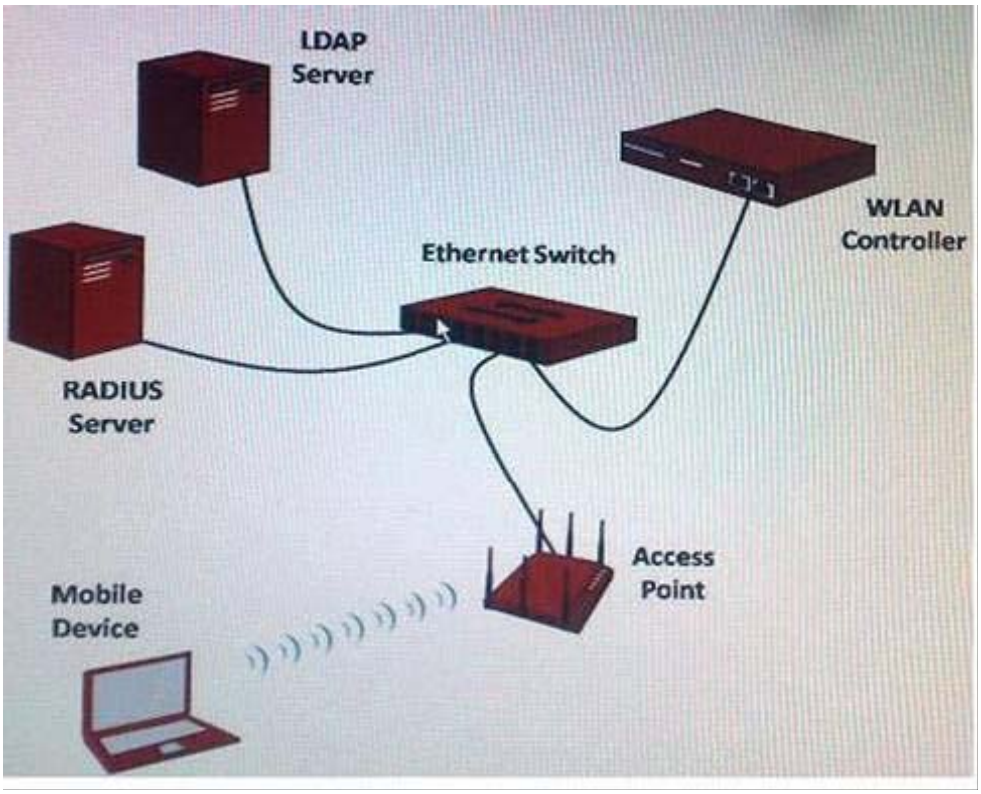
A. This is a TSN and stations may use only the TKIP chiper suit.

B. The BSS's group key chiper will be rotated by the access point after two more beacon frames.

C. The BSS supports both CCMP and TKIP chiper suit simultaneously.
D. There is currently one wireless client associated with the AP using TKIP chiper suit within the BSS.
E. The BSS is an RSN, but the only chiper suit supported in BSS is TKIP.
Answer: E

9.Given: You manage a wireless network that services 200 wireless users. Your facility requires 20 access points and you have installed an IEEE 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. Eavesdropping
B. Offline dictionary
C. Layer 1 DoS
D. Session hijacking
E. Man-in-the-middle
F. Layer 3 peer-to-peer
Answer: B,E
Explanation: LEAP was developed by Cisco in 2001 as an improved version of Extensible Authentication Protocol-MD5 was and it was released as an IEEE 802.1X Extensible Authentication Protocol (EAP) authentication type
LEAP transmits Challenge-Handshake Authentication Protocol (CHAP) negotiations in the open without the benefit of an encrypted tunnel. Thus, LEAP is prone to offline dictionary and brute force attacks
http://www.infinitel00p.com/library/wifisecHTML/WiFi.Security.htm
The systems protected by LEAP are still vulnerable to MITM attacks
http://it.toolbox.com/wiki/index.php/Man-in-the-Middle_Attack

10.Exhibit Given: The network in this diagram implements an 802.1X/EAP-based wireless security solution. What device functions as EAP authenticator?

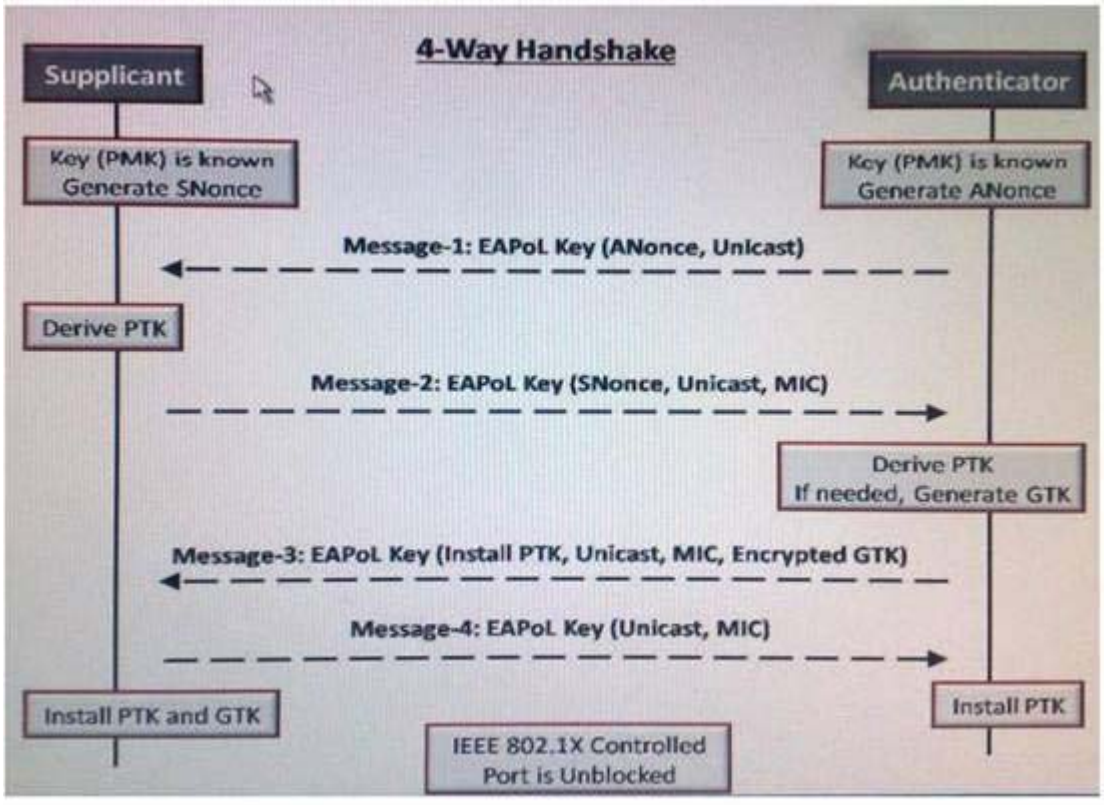


A. Ethernet switch
B. Mobile device
C. LDAP server
D. Access point
E. WLAN controller
F. RADIUS server
Answer: E
Explanation: supplicant is often the laptop or wireless handheld device trying to access the network
A device that blocks or allows traffi c to pass through its port entity. Authentication traffi c is normally allowed to pass through the authenticator, while all other traffi c is blocked until the identity of the supplicant has been verifi ed. The authenticator maintains two virtual ports: anuncontrolled portand acontrolled port. The uncontrolled port allows EAP authentication traffi c to pass through, while the controlled port blocks all other traffi c until the supplicant has been authenticated. In a WLAN, the authenticator is usually either an AP or a WLAN controller.
The authenticator plays the role of the intermediary, passing messages between the supplicant and the authentication server.
In the centralized WLAN architecture, autonomous APs have been replaced with controller - based access points also known as thin APs. Acontroller - based APhas minimal intelligence, and functionally is just a radio card and an antenna. All the intelligence resides in a centralizedWLAN controller, and all the AP confi guration settings, such as channel and power, are distributed to the controller - based APs from the WLAN controller and stored in the RAM of the controller based AP.
In this fig WLAN Controller is used with thin AP therefore the authenticator is WLAN Controller

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

A. EAP-TTLS does not require the use of PKI.
B. EAP-TTLS does not require an authenticator server.
C. EAP-TTLS sends encrypted supplicant credentials to the authentication server.
D. EAP-TTLS supports mutual authentication between supplicants and authentication servers.
E. EAP-TTLS supports smart card clients.
Answer: A
Explanation:
EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extendsTLS. It is widely supported across platforms; although there is no native OS support for this EAP protocol in Microsoft Windows, it requires the installation of small extra programs such as SecureW2. EAPTTLS offers very good security. The client can but does not have to be authenticated via a CA-signed PKI certificate to the server. This greatly simplifies the setup procedure, as a certificate does not need to be installed on every client. http://www.ucertify.com/article/what-is-eap-ttls.html

12.Exhibit



In this diagram illustrating an example of IEEE 802.11standard's4-Way handshake what is the purpose of ANonce and Snonce?
A. There are values used in the derivation of the pairwise Transient key.
B. The IEEE 802.11 standard requires that all crypto graphic frames contain a nonce for security purposes.
C. They are used to pad message 1 and message 2 so each frame contains the same number of bytes.
D. They are added together and used as the GMK, from which the GTK is derived.
E. They allow the participating STAs to avoid sending unicast encryption keys acrossthe wireless medium
Answer: A

13.You own a coffee shop and have recently installed a 802.11g wireless hot spot for the benefit of your customers. For legal reasons you want to minimize your network and avoid liability related to the operations of hot spots.
What option specifies the best approach to achieve this goal at your public hot-spot?
A. Allow only trusted patrons to use the WLAN
B. Use a WIPS to deauthenticate the malicious stations
C. Require clients STAs to have updated firewall and antivirus software
D. Disable the WLAN during non business hours
E. Use the captive portal to force users to agree to an acceptable use disclaimer
F. Configure WPA2-personal security on your access point
G. Block TCP port 25out bound on the internet router
Answer: E
Explanation:
The benefi t of a captive portal over an open SSID is that most networks with captive portals have an acceptable use policy. When the user connects to the captive portal, the acceptable use policy or a link to it is usually displayed on the captive portal page, along with a statement such as " Logging in as a registered user indicates that you have read and accepted the Acceptable Use Policy. " This disclaimer, along with the acceptable use policy,may provide the organization with some legal protection if the user did something illegal while connected to the network. This disclaimer can also give the organization the right to disconnect the user from the network if they violate the rules of the acceptable use policy.

14.Given: XYZ company has recently installed a controller based WLAN and is using a RADIUS server to proxy authenticate request to an LDAP server user based across controls 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 3)
A. The RADIUS server can support vendor-specific attributes in the ACCESS-ACCEPT response which can be used for ASL or firewall assignment.
B. The RADIUS server can communicate with the DHCP server to issue the appropriate IP address and VLAN assignments to users.
C. According to database entries, RADIUS can reassign client 801.11assosiations to proper SSID by referring a user name to SSID mapping
D. RADIUS return list attributes can be used to assign permission level, such as read only permission, to users of particular network source.
E. RADIUS can send a VLAN assignment for each authorized user to the VLAN controller in a return list attribute.
Answer: A,B,E
Explanation: When a RADIUS server provides a successful response to an authentication, the ACCESS - ACCEPT response contains a series of attribute - value pairs (AVPs).Part of the extensibility of RADIUS is the built - in support for adding additional nonreserved AVPs that can be utilized by vendors, called vendor - specifi c attributes page 478, 0470438916.pdf
The IP address of the ACS (RADIUS) server is 172.16.1.1.
The DHCP server address 172.16.1.1 is used to assign the LWAPP to the IP address. The internal DHCP

server on the controller is used to assign the IP address to wireless clients.
Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. This task of assigning users to a specific VLAN is handled by a RADIUS authentication server,
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076
317c.shtml

15.Given: ABC company is developing an IEEE 802.11 complaint wireless security solution using 802.1X/EAP authentication. According to company policy the security should prevent an eavesdropper from decrypting data frames traversing a wireless connection. What security solution features play a role in adhering to this policy requirement? (Choose 2)
A. Group temporal key
B. Message integrity check (MIC)
C. Multi-factor authentication
D. Encrypted passphrase
E. Integrity check value
F. 4-Way handshake
Answer: A,F

16.Given: John smith uses a coffee shop's internet hot spot to transfer funds between his checking and saving accounts at his bank's website. The bank's website uses HTTPS protocol to protect sensitive account information. A hacker was able to obtain john's bank account user ID and password and transfers john's money to another account. How did the hacker obtain john's bank Account user ID and password?
A. John uses same username and password for banking that he does for email. John used a pop3 email client at the wirelesshot-spotto check the email and the user ID and password were not encrypted.
B. The bank's web server is using anX509 certificate that is no signed by a root CA, causing the user ID and password to be sent unencrypted
C. John's bank is using an expiredX509 certificate on there web server. The certificate is on john's certificate Revocation list (CRL), causing the user ID and password to be sent unencrypted.
D. Before connecting to the banks website, johns association to the AP was hijacked. The Attacker interrupted the HTTPS public encryption key from the bank's web server and has decrypted john's login credentials in real time.
E. John accessed his corporate network with the IPSec VPN software at the wirelesshot-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.
Answer: D
Explanation:
Somehot-spots authenticate users. This does not secure the data transmission or prevent packet sniffers from allowing people to see traffic on the network.
http://en.wikipedia.org/wiki/Hot-spot_(Wi-Fi)
The access point software on the attacker ' s laptop is confi gured with the same SSID that is used by a public - accesshot-spot. The attacker ' s access point is now functioning as an evil twin AP with the same SSID but is transmitting on a different channel. The attacker then sends spoofed disassociation or deauthentication frames, forcing client stations associated with thehot-spotaccess point to roam to the evil

twin access point. At this point, the attacker has effectively hijacked wireless clients at Layer 2 from the original access point. Although deauthentication frames are usually used as one way to start a hijacking attack, RF jammers can also be used to force any clients to roam to an evil twin AP.

17.What statement accurately describes the functions of the IEEE 802.1X standard?
A. Port-based access control with support for EAP authentication and AES-CCMP encryption only
B. Port-based access control with encryption key management and distribution
C. Port-based access control with support for authenticated-user VLANs only
D. Port-based access control with 802.3 and 802.11 LANs
E. Port-based access control with permission for three frame types: EAP, DHCP, DNS.
Answer: A
Explanation: the 802.1X standard is a port based access control standard.A Layer 2 authentication protocol called Extensible Authentication Protocol (EAP) is used within the 802.1X framework to validate users at Layer 2.The 802.11 - 2007 standard also requires the use of strong, dynamic encryption - key generation methods. CCMP/AES encryption is the default encryption method, while TKIP/RC4 is an optional encryption method.

18.Company's 500 employees use ABC's dual band HT 802.11 WLAN extensively general data traffic, VoWiFi, and guest access internet-only data. Size and network applications, what solution effects common and recommended security practices for this type of network?
A. His high security requirements, support EAT-TLS for corporate data and VoWiFi, require WPA or WPA2-personal as well as MAC address filtering for all guest solutions. Segment each data type using a separate data type SSID, frequently band, and VLAN.
B. WPA2-Personal for corporate data and VoWiFi application with a long passphrase. For guest access, implementation open authentication. Configure two and VLAN-one for corporate access and one for guest access-and support WMM on the corporate network. For ease-of-use and net work discovery hide the corporate broad cast to the guest SSID.
C. PEAPvO/EAP-MSCHAPv2 for corporate data end VoWiFi, use open authentication with captive portal on the guest network. If the VoWiFi phones can not support, use WPA2-personal with a string passphrase. Segment the three types of traffic by using separate SSIDs and VLANs.
D. WPA2 enterprise for all types of network access. For added configuration simplicity, authenticate all users from a single VLAN but apply filtering with IP ACLs by giving each user to group using RADIUS group attributes. Configure the IPACLs so that each group can only access the necessary resources.
Answer: B
Explanation:
A common strategy, even with newer WLAN controller technology, is to create a guest, voice, and data VLAN. The SSID mapped to the guest VLAN will have limited or no security, and all users are restricted away from network resources and routed off to an Internet gateway. The SSID mapped to the voice VLAN might be using a security solution such a WPA2 - Personal, and the VoWiFi client phones are routed to a VoIP server that provides proprietary QoS services through the VLAN. The SSID mapped to the data VLAN uses a stronger security solution such as WPA2 - Enterprise, and the data users are allowed full access to network resources once authenticated.

19.Given: A VLAN consultant has just finished installing a WLAN controller with 15 controller based APs.

Two SSIDs with separate VLANs are configured for this network and LANs are configured to use the same RADIUS server. The SSIDs are configured as follows
SSID Blue -VLAN 10-lightweight EAP (LEAP) authentication-CCMP cipher suit
SSID Red - VLAN 20-802.1X/PEAPv0 authentication-TKIP cipher suit
The consultants computer can successfully authenticate and browse the internet when using the Blue SSID. The same computer can authenticate when using the Red SSID.
What is most likely cause of problem
A. The consultant does not have a valid Kerberos ID on the Blue VLAN.
B. The TKIP cipher suit is not a valid option for 802.1 X/PEAPv0 authentications.
C. The clock on the consultant's computer post dates the RADIUS server's certificate expiration date/time.
D. PEAPv0 authentication is not supported over controller based access points.
E. The red VLAN does not support certificate based authentication traffic.
Answer: E
Explanation: Microsoft ' sEAP - PEAPv0 (EAP - MSCHAPv2)is the most common form of PEAP. However, it should be noted that EAP - MSCHAPv2 is considered a separate protocol. The credentials used for this version of PEAP are usernames and passwords. Client - side certifi cates are not used and are not supported.

20.After completing the installation of new overlay WIPS, what baseline function MUST be performed?
A. Approved 802.1X/EAP methods need to be selected and confirmed.
B. Configure specifications for upstream and down stream throughout thresholds.
C. Classify the authorized, neighbor, and rogue WLAN devices.
D. Configure profiles for operation among different regularity domains.
Answer: C
Explanation: Most WIDS/WIPS vendors categorize access points and client stations in four or more classifi cations. Wi - Fi vendors may have different names for the various classifi cations, but most solutions classify 802.11 radios as follows:
Authorized Device, Unauthorized Device, Neighbor Device, Rogue Device
Many WIDS/WIPS solutions also have the ability to conductauto - classifi cation. As shown in Figure 10.12, WLAN devices can be automatically added to any classifi cation based on a variety of variables, including authentication method, encryption method, SSID, IP addresses, and so on. Auto - classifi cation capabilities should be used carefully to ensure that only proper devices are classifi ed as authorized.