**802.11 Security Basics**

When you are securing a wireless 802.11 network,

five major components are typically required:

■ Data privacy and integrity

■ Authentication, authorization, and accounting (AAA)

■ Segmentation

■ Monitoring

■ Policy

Because data is transmitted freely and openly in the air, proper protection is needed to ensure data privacy, so strong encryption is needed.

*The wireless portal must be protected, an authentication solution is needed to ensure that only authorized devices and users can pass through the portal via a wireless access point (AP).*

**Data Privacy and Integrity**

All data transmissions travel in the open air, therefore, using cipher encryption technologies we have to provide proper data privacy.

A cipher is an algorithm used to perform encryption.

The two most common algorithms used to protect data are the

* RC4 algorithm
* Advanced Encryption Standard (AES) algorithm.

Some ciphers encrypt data in a continuous stream, whereas others encrypt data in groupings known as blocks.

**RC4 Algorithm** :- The RC4 algorithm is a streaming cipher used in technologies that are often used to protect Internet traffic, such as Secure Sockets Layer (SSL). The RC4 algorithm uses encryption methods known as WEP and TKIP.

**Advanced Encryption Standard Algorithm**:- The AES algorithim is a block cipher that offers much stronger protection than the RC4 streaming cipher. AES uses encryption method known as Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).

The AES algorithm encrypts data in fixed data blocks with choices in encryption key strength of 128, 192, or 256 bits.

*WEP, TKIP and CCMP all use a data integrity check to ensure that the data has not been maliciously altered*.

WEP uses an integrity check value (ICV) and TKIP uses a message integrity check (MIC). CCMP also uses a message integrity check (MIC) that is much stronger than the data integrity methods used in TKIP or WEP.

**Authentication, Authorization, and Accounting**

**Authentication** :- Authentication is the verification of identity and credentials. Users or devices must identify themselves and present credentials, such as usernames and passwords or digital certificates. More secure authentication systems use multifactor authentication, which requires at least two sets of different types of credentials to be presented.

**Authorization**:- Authorization determines if the device or user is authorized to have access to network resources. This can include identifying whether you can have access based upon the type of device you are using (laptop, tablet, or phone), time of day restrictions, or location. Before authorization can be determined, proper authentication must occur.

**Accounting**:- Accounting is tracking the use of network resources by users and devices. A record is kept of user identity, which resource was accessed, and at what time.

**Segmentation**

It can be achieved through a variety of means, including firewalls, routers, VPNs, and VLANs. The most common wireless segmentation strategy used in 802.11 enterprise WLANs is segmentation using virtual LANs (VLANs). Segmentation is also intertwined with role-based access control (RBAC).

**Legacy Authentication**

The original 802.11 standard specified two methods of authentication:

Open System authentication and Shared Key authentication.

Validating the identity of a user when they are connecting or logging onto a network.

802.11 authentication is very different from this. These legacy authentication methods were not so much an authentication of user identity, but more of an authentication of capability.

Think of these authentication methods as verification between the two devices that they are both valid 802.11 devices.

***Open System authentication*** provides authentication without performing any type of user verification.

It is essentially a two-way exchange between the client radio and the access point:

1. The client sends an authentication request.

2. The access point then sends an authentication response. Because Open System authentication does not require the use of any credentials, every client gets authenticated and therefore authorized onto network resources after they have been associated.

Static WEP encryption is optional with Open System authentication and may be used to encrypt the data frames after Open System authentication and association occur.

***Shared Key authentication*** used Wired Equivalent Privacy (WEP) to authenticate client stations and required that a static WEP key be configured on both the station and the access point. In addition to WEP being mandatory, authentication would not work if the static WEP keys did not match.

Shared Key authentication was a four-way authentication frame handshake:

1. The client station sent an authentication request to the access point.

2. The access point sent a cleartext challenge to the client station in an authentication response.

3. The client station encrypted the cleartext challenge and sent it back to the access point in the body of another authentication request frame.

4. The access point decrypted the station’s response and compared it to the challenge text:

■ If they matched, the access point would respond by sending a fourth and final authentication frame to the station confirming the success.

■ If they did not match, the access point would respond negatively. If the access point could not decrypt the challenge, it would also respond negatively.

If Shared Key authentication was successful, the same static WEP key that was used during the Shared Key authentication process would also be used to encrypt the 802.11 data frames.

**MAC Filters**

Most vendors provide MAC filtering capabilities on their access points. *MAC filters can be configured to either allow or deny traffic from specific client MAC addresses* to associate and connect to an AP.

The 802.11 standard does not define MAC filtering, and any implementation of MAC filtering is vendor specific.

*Most vendors use MAC filters to deny client associations to an AP.*

Hacker can easily bypass any MAC filter by spoofing an allowed client MAC address. MAC filtering is not considered a reliable means of security for wireless enterprise networks.

**SSID Cloaking**

Access points typically have a setting called Closed Network or Broadcast SSID.

By either enabling a closed network or disabling the broadcast SSID feature, you can hide, or cloak, your wireless network name.

*When you implement a closed network, the SSID field in the beacon frame is null (empty), and therefore passive scanning will not reveal the SSID to client stations that are listening to beacons.*

The SSID, which is also often called the ESSID, is the logical identifier of a WLAN.

Many wireless client software utilities transmit probe requests with null SSID fields when actively scanning for access points.

When you implement a closed network, the access point responds to null probe requests with probe responses; however, as in the beacon frame, the SSID field is null, and therefore the SSID is hidden to client stations that are using active scanning.

*Effectively, your wireless network is temporarily invisible, or cloaked. Note that an access point in a closed network will respond to any configured client station that transmits directed probe requests with the properly configured SSID.*

This ensures that legitimate end users will be able to authenticate and associate to the AP.

However, any client stations that are not configured with the correct SSID will not be able to authenticate or associate. Although implementing a closed network may hide your SSID from some of these WLAN discovery tools, anyone with a layer 2 wireless protocol analyzer can capture the frames transmitted by any legitimate end user and discover the SSID, which is transmitted in cleartext. In other words, a hidden SSID can be found usually in seconds with the proper tools. Many wireless professionals will argue that hiding the SSID is a waste of time, whereas others view a closed network as just another layer of security

**Robust Security**

The 802.11 standard defines an enterprise authentication method as well as a method of authentication for home use.

The current standard defines the use of an 802.1X/EAP authentication and also the use of a *preshared key (PSK) or a passphrase.*

The 802.11 standard also requires the use of strong, dynamic encryption-key generation methods.

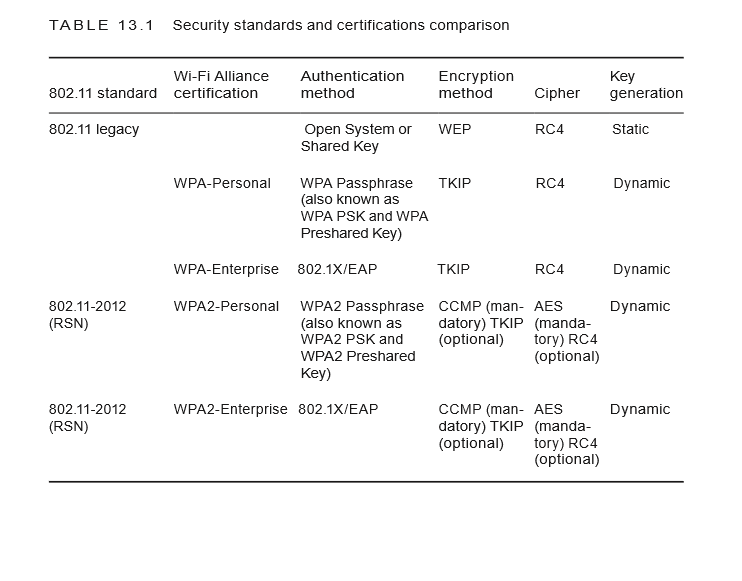
CCMP/AES encryption is the default encryption method, and TKIP/RC4 is an optional encryption method.

Wi-Fi Protected Access (WPA) certification supporting only TKIP/RC4 dynamic encryption-key generation.

802.1X/EAP authentication was intended for the enterprise, and passphrase authentication was suggested in a SOHO environment.

After Introduced the WPA2 certification., WPA2 supports both CCMP/ AES and TKIP/RC4 dynamic encryption-key generation. 802.1X/EAP authentication is more complex and meant for the enterprise, whereas passphrase authentication is simpler and meant for a SOHO environment.

Table 13.1 offers a valuable comparison of the various security standards and certifications.



**Robust Security Network (RSN)**

The 802.11 standard defines what are known as a robust security network (RSN) and robust security network associations (RSNAs).

*Two stations (STAs) must authenticate and associate with each other, as well as create dynamic encryption keys through a process known as the 4-Way Handshake. This association between two stations is referred to as an RSNA.*

In other words, any two radios must share dynamic encryption keys that are unique between those two radios. CCMP/AES encryption is the mandated encryption method, and TKIP/RC4 is an optional encryption method. A robust security network (RSN) is a network that allows for the creation of only robust security network associations (RSNAs).

An RSN can be identified by a field found in beacons, probe response frames, association request frames, and reassociation request frames. This field is known as the RSN Information Element (IE). This field may identify the cipher suite capabilities of each station.

The 802.11-2012 standard does allow for the creation of pre–robust security network associations (pre-RSNAs) as well as RSNAs. In other words, legacy security measures can be supported in the same basic service set (BSS) along with RSN-security-defined mechanisms. A transition security network (TSN) supports RSN-defined security, as well as legacy security such as WEP, within the same BSS, although most vendors do not support a TSN.

**PSK Authentication**

The 802.11 standard defines authentication and key management (AKM) services.

AKM services require both authentication processes and the generation and management of encryption keys.

The protocol it uses are preshared (PSK) or an EAP protocol used during 802.1X authentication.

802.1X/EAP requires a RADIUS server and advanced skills to configure and support it. The average home or small business Wi-Fi user has no knowledge of 802.1X/EAP and does not have a RADIUS server in their living room.

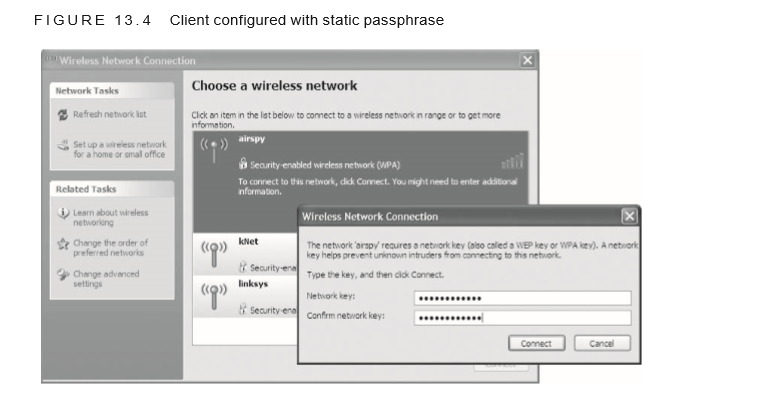
PSK authentication is meant to be used in SOHO environments. Therefore, the security used in SOHO environments is PSK authentication.

*WPA/WPA2Personal utilizes PSK authentication. On the other hand, WPA/WPA2-Enterprise refers to the 802.1X/EAP authentication solution.*

The intended goal of WPA-Personal was to move away from static encryption keys to dynamically generated keys using a simple passphrase as a seed.

WPA/WPA2-Personal allows an end user to enter a simple ASCII character string, dubbed a passphrase, anywhere from 8 to 63 characters in size.

Behind the scenes, *a passphrase-to-PSK-mapping function* takes care of the rest. Therefore, all the user has to know is a single, secret passphrase to gain access to the WLAN, as shown in Figure 13.4.



, the only practical difference between WPA and WPA2 has to do with the encryption cipher. *WPA-Personal and WPA2-Personal both use the PSK authentication method; however, WPA-Personal specifes TKIP/RC4 encryption and WPA2-Personal specifies CCMP/AES.*

TKIP encryption has slowly been phased out over the years and is not supported for any of the 802.11n and 802.11ac data rates. In other words, older 802.11a/b/g radios that support only WPA-Personal and TKIP might still be deployed.

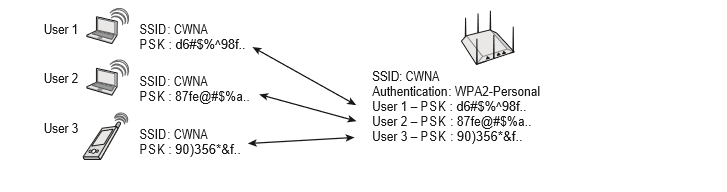
**Note**:-If PSK authentication is the chosen security method, WPA2-Personal should always be used.

Note:- The biggest problem with using PSK authentication in the enterprise is social engineering. The PSK is the same on all WLAN devices. If an end user accidentally gives the PSK to a hacker, WLAN security is compromised. If an employee leaves the company, to maintain a secure environment all of the devices have to be reconfigured with a new 256-bit PSK. Because the passphrase or PSK is shared by everyone, a strict policy should be mandated stating that only the WLAN security administrator is aware of the passphrase or PSK. That, of course, creates another administrative problem because of the work involved in manually configuring each device.

Several enterprise WLAN vendors have come up with a creative solution to using WPA/ WPA2-Personal that solves some of the biggest problems of using a single passphrase for WLAN access.

Each computing device or user will have their own unique PSK for the WLAN. Individual users can be mapped to a unique WPA/WPA2-Personal passphrase. A database of unique PSKs mapped to usernames or client stations must be stored on all access points or on a centralized WLAN controller. Individual users are then assigned a unique PSK that is created either dynamically or manually.

As shown in Figure 13.5, the authenticator maintains a database of each individual PSK for each individual client. The PSKs that are generated can also have an expiration date. Unique time-based PSKs can also be used in a guest WLAN environment as a replacement for more traditional username/ password credentials.



**802.1X/EAP Framework**

The 802.1X standard is a port-based access control standard.

**802.1X provides an authorization framework that allows or disallows traffic to pass through a port and thereby access network resources.**

An 802.1X framework may be implemented in either a wireless or wired environment.

The 802.1X framework consists of three main components:

**Supplicant**

A host with software that requests authentication and access to network resources is known as a supplicant. Each supplicant has unique authentication credentials that are verified by the authentication server.

**Authenticator**

An authenticator device blocks traffic or allows traffic to pass through its port entity. Authentication traffic is normally allowed to pass through the authenticator, whereas all other traffic is blocked until the identity of the supplicant has been verified.

The authenticator maintains two virtual ports: an uncontrolled port and a controlled port. The uncontrolled port allows EAP authentication traffic to pass through, and the controlled port blocks all other traffic until the supplicant has been authenticated.

**Authentication Server (AS)**

The authentication server (AS) maintains a user database or may proxy with an external database, such as an LDAP database, to authenticate user credentials.

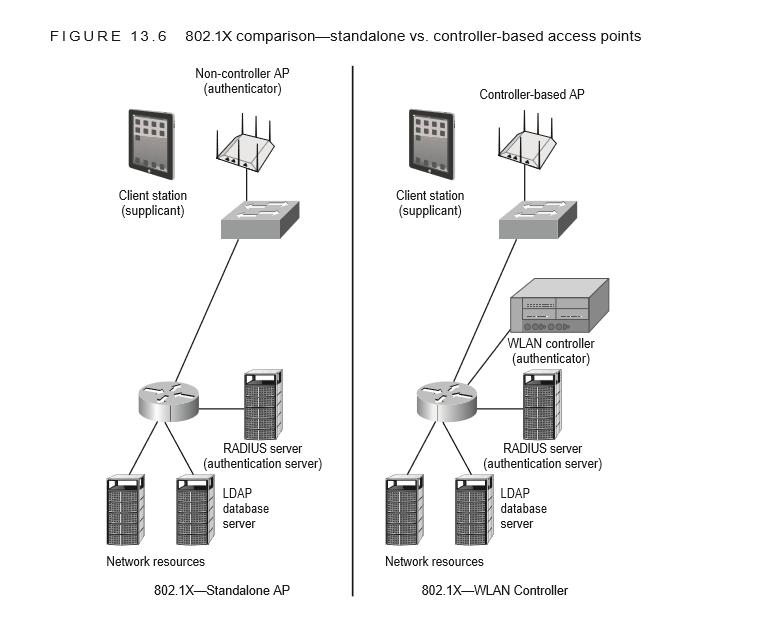
As seen in Figure 13.6, a standalone access point would be the authenticator, blocking access via virtual ports, and the AS is typically an external RADIUS server.

Figure 13.6 also shows that when an 802.1X security solution is used with a WLAN controller solution, the WLAN controller is typically the authenticator—and not the controller-based access points.

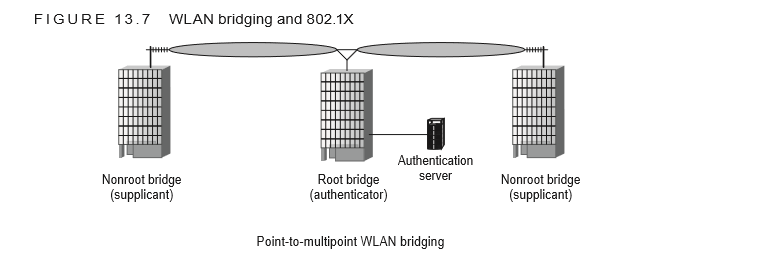
In either case, directory services are often provided by a Lightweight Directory Access Protocol (LDAP) database that the RADIUS server communicates with directly.

Active Directory would be an example of an LDAP database that is queried by a RADIUS server.

Note that some WLAN vendors offer solutions where either a standalone AP or a WLAN controller can dual-function as a RADIUS server and perform direct LDAP queries, thus eliminating the need for an external RADIUS server.



As you can see in Figure 13.7, the root bridge would be the authenticator and the nonroot bridge would be the supplicant if 802.1X security is used in a WLAN bridged network.



An authentication protocol is needed to perform the authentication process.

Extensible Authentication Protocol (EAP) is used to provide user authentication. EAP is a flexible layer 2 authentication protocol used by the supplicant and the authentication server to communicate.

The authenticator allows the EAP traffic to pass through its virtual uncontrolled port.After the authentication server has verified the credentials of the supplicant, the server sends a message to the authenticator that the supplicant has been authenticated; the authenticator is then authorized to open the virtual controlled port and allow all other traffic to pass through.

**EAP Types**

EAP stands for Extensible Authentication Protocol. EAP is a layer 2 protocol that is very flexible, and many different flavors of EAP exist.

Some, such as Cisco’s Lightweight Extensible Authentication Protocol (LEAP), are proprietary, whereas others, such as Protected Extensible Authentication Protocol (PEAP), are considered standards based.

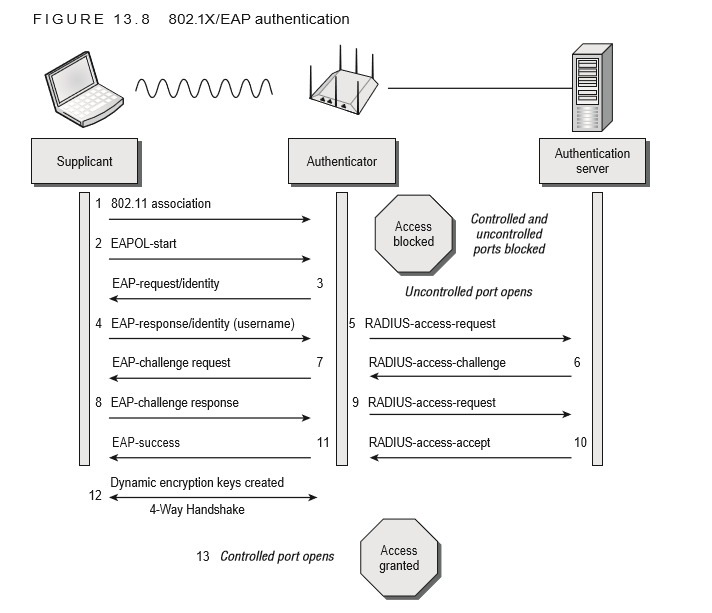
Some provide for only one-way authentication; others provide two-way authentication. ***Mutual authentication not only requires that the authentication server validate the client credentials, but the supplicant must also authenticate the validity of the authentication server.***

By validating the authentication server, the supplicant can ensure that the username and password are not inadvertently given to a rogue authentication server.

Most types of EAP that require mutual authentication use a server-side digital certificate to validate the authentication server. A server-side certificate is installed on the RADIUS server, while the certificate authority (CA) root certificate resides on the supplicant.

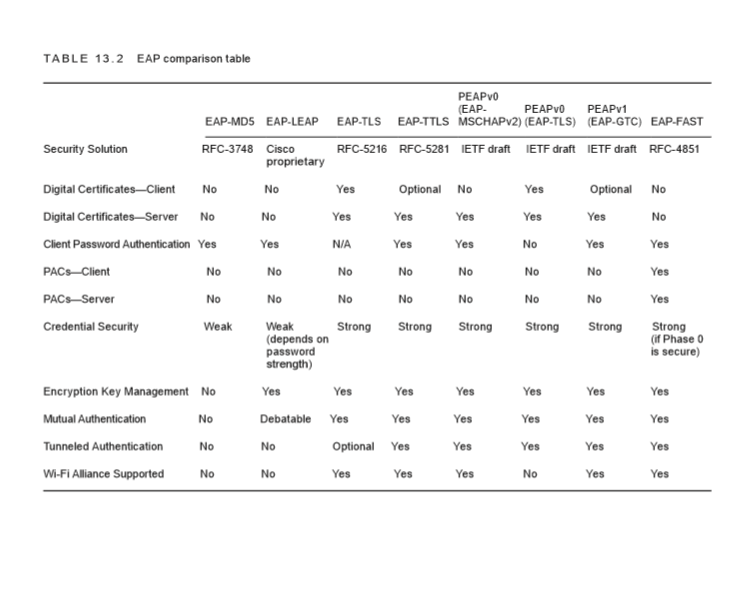
The certificate exchange also creates an encrypted Secure Sockets Layer (SSL) / Transport Layer Security (TSL) tunnel in which the supplicant’s username/password credentials or client certificate can be exchanged.

Many of the secure forms of EAP use tunneled authentication. The SSL/TLS tunnel is used to encrypt and protect the user credentials during the EAP exchange.



**Dynamic Encryption-Key Generation**

Although the 802.1X/EAP framework does not require encryption, the use of encryption is recommended.



However 802.1X/EAP is the generation and distribution of dynamic encryption keys.

EAP protocols that utilize mutual authentication provide “seeding material” that can be used to generate encryption keys dynamically.

Until now, you have learned about only static WEP keys. The use of static keys is typically an administrative nightmare, and when the same static key is shared among multiple users, the secret is easy to compromise via social engineering.

The advantage of dynamic keys is that every user has a different and unique key that cannot be compromised by social engineering attacks. After an EAP frame exchange where mutual authentication is required, both the AS and the supplicant know information about each other because of the exchange of credentials. This newfound information is used as seeding material or keying material to generate a matching dynamic encryption key for both the supplicant and the authentication server.

These dynamic keys are generated per session per user, meaning that every time a client station authenticates, a new key is generated and every user has a unique and separate key.

**Dynamic WEP Encryption**

Please understand that a dynamic WEP key is not the same as TKIP or CCMP encryption keys that are also generated dynamically. WPA/WPA2 security deﬁes the creation of stronger and safer dynamic TKIP/RC4 or CCMP/AES encryption keys that are also generated as a by-product of the EAP authentication process.

**4-Way Handshake**

RSNAs utilize a dynamic encryption-key management method that involves the creation of five separate keys.

Part of the RSNA process involves the creation of two master keys known as the Group Master Key (GMK) and the Pairwise Master Key (PMK).

The PMK is created as a result of the 802.1X/EAP authentication.These master keys are the seeding material used to create the final dynamic keys that are used for encryption and decryption.

The final encryption keys are known as the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK).

The PTK is used to encrypt/decrypt unicast traffic, and the GTK is used to encrypt/decrypt broadcast and multicast traffic. These final keys are created during a four-way EAP frame exchange that is known as the 4-Way Handshake.

*Whenever TKIP/RC4 or CCMP/AES dynamic keys are created, the 4-Way Handshake must occur.*

*Also, every time a client radio roams from one AP to another, a new 4-Way Handshake must occur so that new unique dynamic keys can be generated*

**WPA/WPA2-Personal**

Do you have a RADIUS server in your home or small business? The answer to that question will almost always be no. If you do not own a RADIUS server, 802.1X/EAP authentication will not be possible.

WPA/WPA2-Enterprise solutions require 802.1X for mutual authentication using some form of EAP. Additionally, an authentication server will be needed. Because most of us do not have a RADIUS server in our basement, the 802.112012 standard offers a simpler method of authentication using a PSK. This method involves manually typing matching passphrases on both the access point and all client stations that will need to be able to associate to the wireless network.

A formula is run that converts the passphrase to a Pairwise Master Key (PMK) used with the 4-Way Handshake to create the final dynamic encryption keys. This simple method of authentication and encryption key generation is known as WPA/ WPA2-Personal.

Other names include WPA/WPA2 Preshared Key and WPA/WPA2 PSK. Although this is certainly better than static WEP and Open System authentication, WPA/ WPA2-Personal still requires signifcant administrative overhead and has potential social engineering issues in a corporate or enterprise environment.

An 802.1X/EAP solution as defned by WPA/WPA2Enterprise is the preferred method of security in a corporate and workplace environment.

**TKIP Encryption**

*The optional encryption method defined for a robust security network is Temporal Key Integrity Protocol (TKIP).* This method uses the RC4 cipher just as WEP encryption does. As a matter of fact, TKIP is an enhancement of WEP encryption that addresses many of the known weaknesses of WEP.

TKIP starts with a 128-bit temporal key that is combined with a 48-bit initialization vector (IV) and source and destination MAC addresses in a complicated process known as per-packet key mixing.

This key-mixing process mitigates the known IV collision and weak key attacks used against WEP.

TKIP also uses a sequencing method to mitigate the reinjection attacks used against WEP. Additionally, TKIP uses a stronger data integrity check known as the message integrity check (MIC) to mitigate known bit-flipping attacks against WEP.

All TKIP encryption keys are dynamically generated as a final result of the 4-Way Handshake.

WEP encryption adds an extra 8 bytes of overhead to the body of an 802.11 data frame. When TKIP is implemented, because of the extra overhead from the extended IV and the MIC, a total of 20 bytes of overhead is added to the body of an 802.11 data frame.

The 802.11n and higher amendments do not permit the use of WEP encryption or TKIP encryption for the High Throughput (HT) and Very High Throughput (VHT) data rates. The Wi-Fi Alliance will only certify 802.11n radios that use CCMP encryption for the higher data rates. For backward compatibility, newer radios will still support TKIP and WEP for the slower data rates defined for legacy 802.11a/b/g radios.

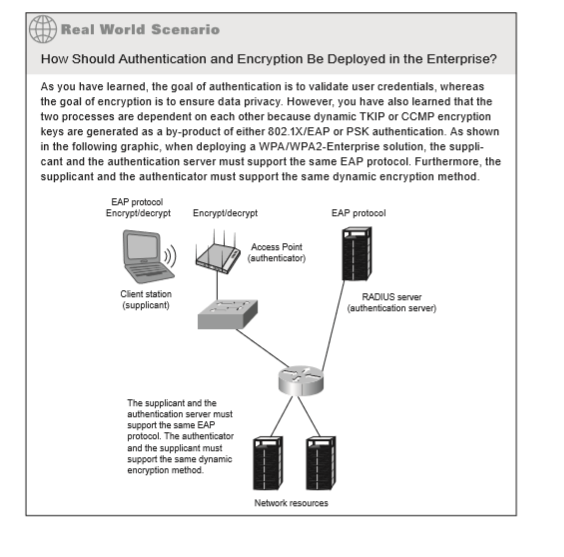
**CCMP Encryption**

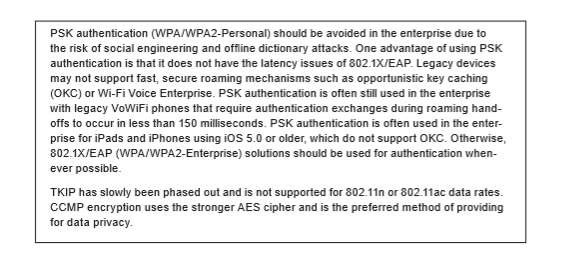
The default encryption method defined under the 802.11i amendment is known as Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). This method uses the Advanced Encryption Standard (AES) algorithm .

CCMP/AES uses a 128-bit encryption-key size and encrypts in 128-bit fixed-length blocks. An 8-byte message integrity check (MIC) is used that is considered much stronger than the one used in TKIP.

Also, because of the strength of the AES cipher, per-packet key mixing is unnecessary. All CCMP encryption keys are dynamically generated as a final result of the 4-Way Handshake. CCMP/AES encryption will add an extra 16 bytes of overhead to the body of an 802.11 data frame.

Because the AES cipher is processor intensive, older legacy 802.11 devices do not have the processing power necessary to perform AES calculations. Older 802.11 devices cannot be firmware upgraded, and a hardware upgrade is needed to support WPA2.





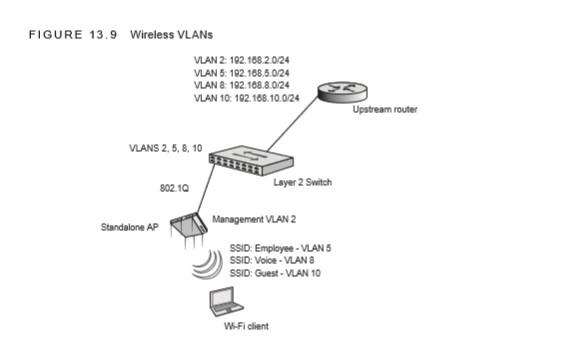
**Traffic Segmentation**

Segmentation is a key part of a network design. Once authorized onto network resources, user traffic can be further restricted as to what resources may be accessed and where user traffic is destined. Segmentation can be achieved through a variety of means, including firewalls, routers, VPNs, and VLANs. A common wireless segmentation strategy used in 802.11 enterprise WLANs is layer 3 segmentation that employs VLANs mapped to different subnets. Segmentation is also often intertwined with role-based access control (RBAC).

**VLANs**

In a WLAN environment, individual SSIDs can be mapped to individual VLANs, and users can be segmented by the SSID/VLAN pair, all while communicating through a single access point.

Each SSID can also be configured with separate security settings. Most enterprise access points have the ability to broadcast as many as 16 SSIDs and each SSID can be mapped to a unique VLAN.



The SSID mapped to the guest VLAN often is an open SSID, although all guest users should be restricted via a firewall policy. Guest users are denied access to local network resources and routed off to an Internet gateway.

Voice SSID/VLAN

The voice SSID might be using a security solution, such as a WPA2 Passphrase, and the VoWiFi client traffic is typically routed to a VoIP server or private branch exchange (PBX).

Employee SSID/VLAN

The employee SSID uses a stronger security solution, such as WPA2-Enterprise, and access control lists (ACLs) or firewall policies allow the employees to access full network resources once authenticated.

The user VLANs are not available at the access layer switch. The controller-based APs are connected to an access port of the edge switch. The user VLANs are still available to the wireless users because all of the user VLANs are encapsulated in an IP tunnel between the controller-based APs at the edge and the WLAN controller in the core.

When cooperative APs or autonomous APs are deployed, all of the user VLANs are confi gured in the access layer switch.

The standalone access points are connected to an 802.1Q trunk port of the edge switch. The user VLANS are tagged in the 802.1Q trunk and all wireless user traffic is forwarded at the edge of the network.

**RBAC**

Role-based access control (RBAC) is another approach to restricting system access to authorized users.

Many of the WLAN vendors provide RBAC capabilities.

The three main components of an RBAC approach are users, roles, and permissions.

Separate roles can be created, such as a sales role or a marketing role. Individuals or groups of users are assigned to one of these roles.

Permissions can be defined as layer 2 permissions (VLANS or MAC filters), layer 3 permissions (access control lists), layers 4–7 permissions (stateful firewall rules), and bandwidth permissions.

For example, users who associate with a “Guest” SSID are placed in a unique guest VLAN. The users then authenticate via a captive portal and are assigned a guest role. The guest role may have bandwidth permissions that restrict them to 100 kbps of bandwidth and allow them to use only ports 80 (HTTP), 443 (HTTPS), 25 (SMTP), and 110 (POP) during working hours. This scenario would restrict guest users who are accessing the Internet from hogging bandwidth and only allow them to view web pages and check email between 9 a.m. and 5 p.m.

**Interface Security**

Enterprise equipment usually can be configured either through a command-line interface or a web interface or via Simple Network Management Protocol (SNMP).

Any interface that is not used should be turned off*. For example, if the administrator confi gures the access points only via a command-line interface (CLI), turn off the web interface capabilities on the access points.*

At a minimum, all the passwords for these configuration options should be changed from the factory defaults. Keep in mind that some management interfaces have multiple default user levels. The default levels can include administrator, guest, and management. The passwords for all of these levels should be changed. Most infrastructure devices should also support some type of encrypted management capabilities.

Newer Wi-Fi hardware should support SSH, HTTPS, or SNMPv3. Older legacy equipment may not support encrypted login capabilities. It is also a highly recommended practice to configure your infrastructure devices from only the wired side and never configure them wirelessly, although with more organizations replacing their wired networks in favor of wireless networks, this may not be feasible.

If devices are configured from the wireless side, an intruder might be able to capture your wireless packets and be able to watch what you are doing. If wireless management is allowed, it should be restricted to secured SSIDs only.

An access point will broadcast an emergency WPA2-Personal SSID that is triggered by the loss of IP connectivity between the AP and the default gateway. An administrator can then securely connect to the emergency SSID and create a wireless console connection to the CLI of the AP. This provides a method for the admin to identify why layer 3 connectivity was lost without having to climb a ladder to connect to the console port of the AP.

**VPN Wireless Security**

Although the 802.11 standard clearly defines layer 2 security solutions, the use of upper-layer virtual private network (VPN) solutions can also be deployed with WLANs.

VPNs are typically not recommended to provide wireless security in the enterprise due to the overhead and because faster, more secure layer 2 solutions are now available. Although not usually a recommended practice,

VPNs were often used for WLAN security because the VPN solution was already in place inside the wired infrastructure. VPNs do have their place in Wi-Fi security and should defi nitely be used for remote access. They are also sometimes used in wireless bridging environments.

The two major types of VPN topologies are

router-to-router or client-server based.

Use of VPN technology is mandatory for remote access. Your end users will take their laptops off site and will most likely use public access Wi-Fi hotspots. Because there is no security at most hotspots, a VPN solution is needed. The VPN user will need to bring the security to the hotspot in order to provide a secure, encrypted connection. It is imperative that users implement a VPN solution coupled with a personal firewall whenever accessing any public access Wi-Fi networks.

**Layer 3 VPNs**

VPNs have several major characteristics. They provide encryption, encapsulation, authentication, and data integrity.

*VPNs use secure tunneling, which is the process of encapsulating one IP packet within another IP packet.*

The first packet is encapsulated inside the second or outer packet. The original destination and source IP address of the first packet is encrypted along with the data payload of the first packet.

VPN tunneling, therefore, protects your original private layer 3 addresses and also protects the data payload of the original packet. Layer 3 VPNs use layer 3 encryption; therefore, the payload that is being encrypted is the layer 4–7 information. The IP addresses of the second or outer packet are seen in cleartext and are used for communications between the tunnel endpoints. The destination and source IP addresses of the second or outer packet will point to the public IP address of the VPN server and VPN client software.

The most commonly used layer 3 VPN technology is Internet Protocol Security (IPsec). IPsec VPNs use stronger encryption methods and more secure methods of authentication and are the most commonly deployed VPN solution. IPsec supports multiple ciphers, including DES, 3DES, and AES. Device authentication is achieved by using either a serverside certificate or a preshared key.

IPsec VPNs require client software to be installed on the remote devices that connect to a VPN server. Most IPsec VPNS are NAT-transversal, but any firewalls at a remote site require (at a minimum) that UDP ports 4500 and 500 be open.

**SSL VPN**

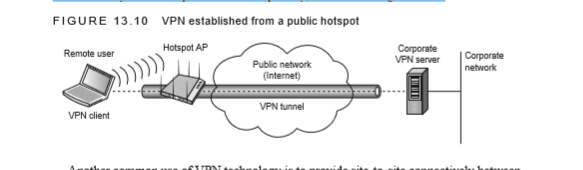
VPN technologies do exist that operate at other layers of the OSI model, including SSL tunneling. Unlike an IPsec VPN, an SSL VPN does not require the installation and confi guration of client software on the end user’s computer.

A user connects to a Secure Sockets Layer (SSL) VPN server via a web browser. The traffic between the web browser and the SSL VPN server is encrypted with the SSL protocol or Transport Layer Security (TLS).

TLS and SSL encrypt data connections above the Transport layer, using asymmetric cryptography for privacy and a keyed message authentication code for message reliability. Although most IPsec VPN solutions are NAT-transversal, SSL VPNs are often chosen because of issues with NAT or restrictive firewall policies at remote locations.

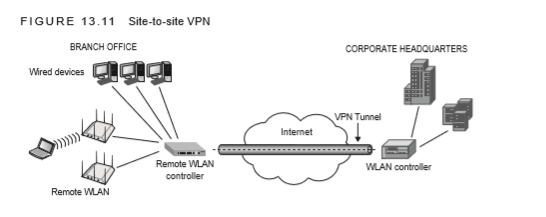
**VPN Deployment**

VPNs are most often used for client-based security when connected to public access WLANs and hotspots that do not provide security. Because most hotspots do not provide layer 2 security, it is imperative that end users provide their own security. VPN technology can provide the necessary level of security for remote access when end users connect to public access WLANs. Since no encryption is used at public access WLANs, a VPN solution is usually needed to provide for data privacy, as shown in Figure 13.10.



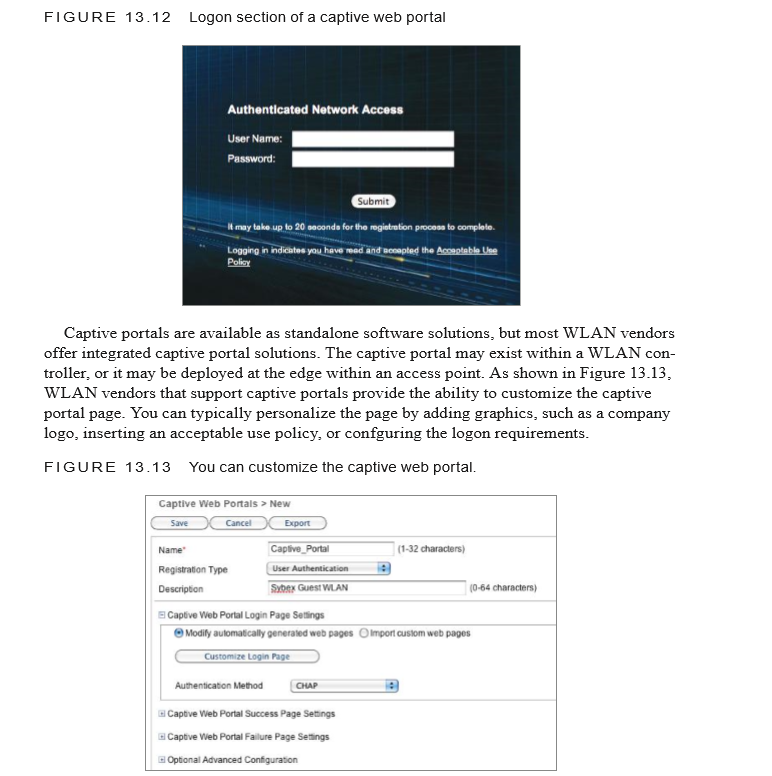
Another common use of VPN technology is to provide site-to-site connectively between a remote office and a corporate office. Most WLAN vendors now offer VPN client-server capabilities in either their APs or WLAN controllers.

As shown in Figure 13.11, a branch office WLAN controller with VPN capabilities can tunnel WLAN client traffic and bridged wired-side traffic back to the corporate network. Other WLAN vendors can also tunnel user traffic from a remote AP to a VPN server gateway.



**Captive Portal**

Most hotspots and guest networks are secured by a captive portal. A captive portal is essentially the integration of a firewall with an authentication web page. Although captive portals are often associated with hotspots and wireless guest networks, the technology is not specifically affiliated with wireless networks. When a user connects to the guest network, whether wired or wireless, any packets that the user transmits are intercepted and blocked from accessing a gateway to the network resources until the user has authenticated through the captive portal. Figure 13.12 shows the logon section of a captive portal web.



Authenticating to a captive portal typically requires the user to enter a username and password. This username and password are verified against a RADIUS database. If the username and password are valid, the user is then allowed to access other resources, such as the Internet. A firewall policy normally restricts the guest users from any corporate resources but gives the users access to an Internet gateway. Not all captive portal pages require a username and password for authentication. Some vendors have begun to use unique dynamic PSKs as user credentials. A guest management solution that utilizes unique PSKs as credentials also provides data privacy for guest users with WPA2 encryption. Some organizations deploy a guest WLAN where the captive web portal does not require any credentials whatsoever. Captive web portals that do not require credentials still provide an acceptable use policy, which functions as a legal disclaimer for the guest network

Security Measures Link layer (layer 2) security protocols are used directly between wireless stations and the access point.

Cipher suites include CCMP, TKIP, and WEP.

CCMP uses an AES block cipher, and TKIP and WEP use an RC4 stream cipher.

Authentication and key management generally takes the form of 802.1X/EAP and RADIUS elements. EAP types may include EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-LEAP, and many others.

Pre-Shared Keys

WEP and WPA-PSK are examples of data link layer wireless security protocols where a persistent shared key is used between the access point and the client device. The pre-shared key is manually configured into the client utility software and into the access points firmware.

This key is used for all station pairs in an ESS and for many successive sessions before being changed, if ever. Once authenticated, a station pair link is secured using the RC4 or AES encryption algorithms. Once a data link is secured, a protocol analyzer will display WEP Data for encrypted data frames.

Some wireless protocol analyzers have the ability to decrypt frames encrypted with pre-shared keys by entering the pre-shared key into the analyzer software. Most analyzers support this function using static WEP keys, and some products are now capable of performing this task with WPA-PSK.

802.1X/EAP

There are numerous EAP types on the market today, and each works slightly different. There are advantages and disadvantages to each.

Figures 9.15 and 9.16 illustrate two frame captures of 802.1X/EAP-PEAP-MS-CHAPv2. The first capture is an implementation from one vendor, and the second capture is an implementation from another vendor. One vendor completes the PEAP authentication in 58 packets (including ACKs) and gives an anonymous username that can be viewed in clear text with an analyzer as shown in Figure 9.15.

This anonymous user name is entered into the client software by the user of the client device. The other vendor completes the PEAP authentication in 38 packets (including ACKs) and allows the real user name to be transmitted in clear text as shown in Figure 9.16.

