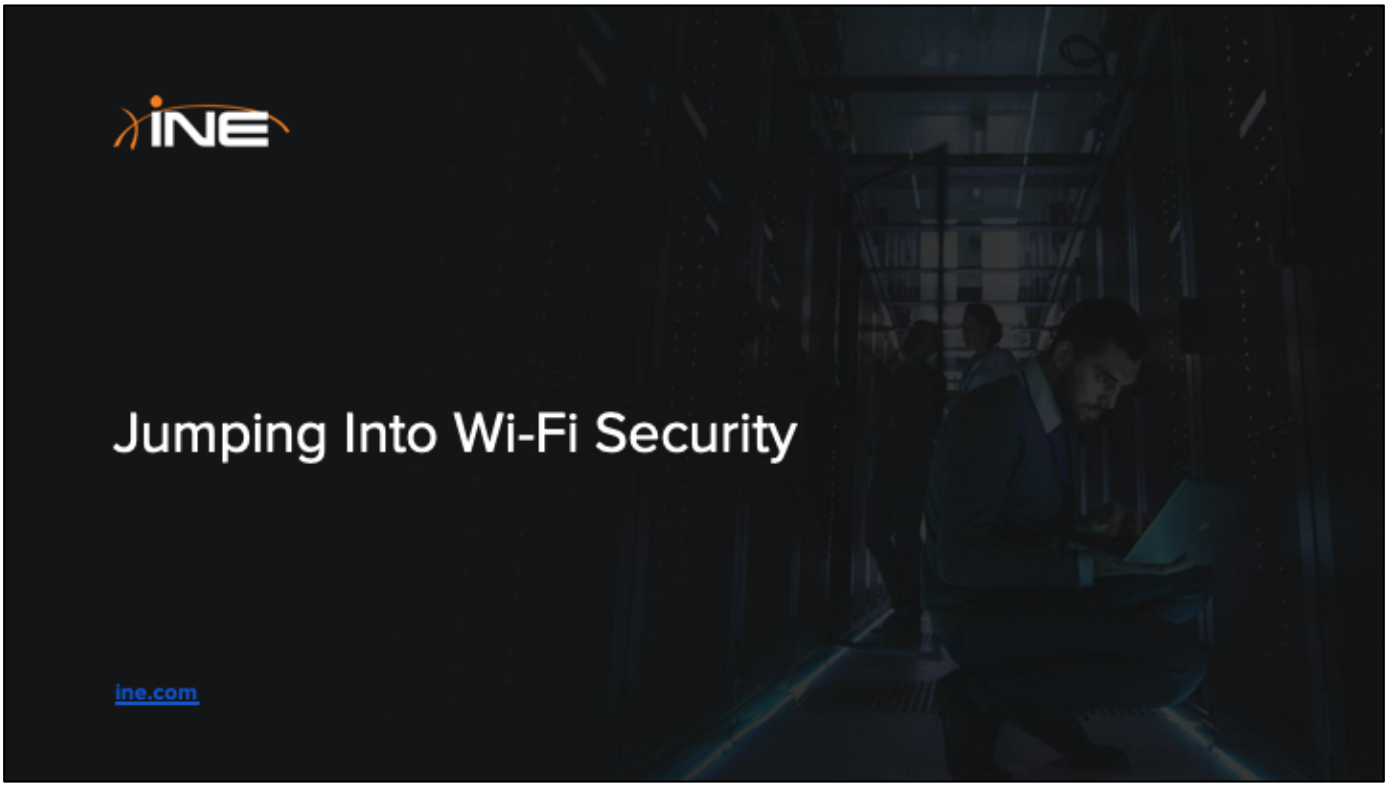

Jumping Into Wi-Fi Security
ine.com


Keith Bogart
CCIE #4923
kbogart@ine.com
@keithbogart1
linkedin.com/in/keith-bogart-2a75042
CCIE Routing & Switching

Course Prerequisites

- Basic understanding of security principles such as encryption & authentication
- Familiarity with WLAN concepts such as SSID, APs and Controllers

Course Objectives

- Summarize why WLAN security is important
- Identify secured & unsecured WLANs
- List the different methods available for WLAN authentication on unsecured networks.
- Explain differences between WEP, WPA, WPA2 & WPA3
- Configure autonomous access points & Controller SSIDs for WPA2 security with PSK


The Need For & Components Of
WLAN Security
ine.com

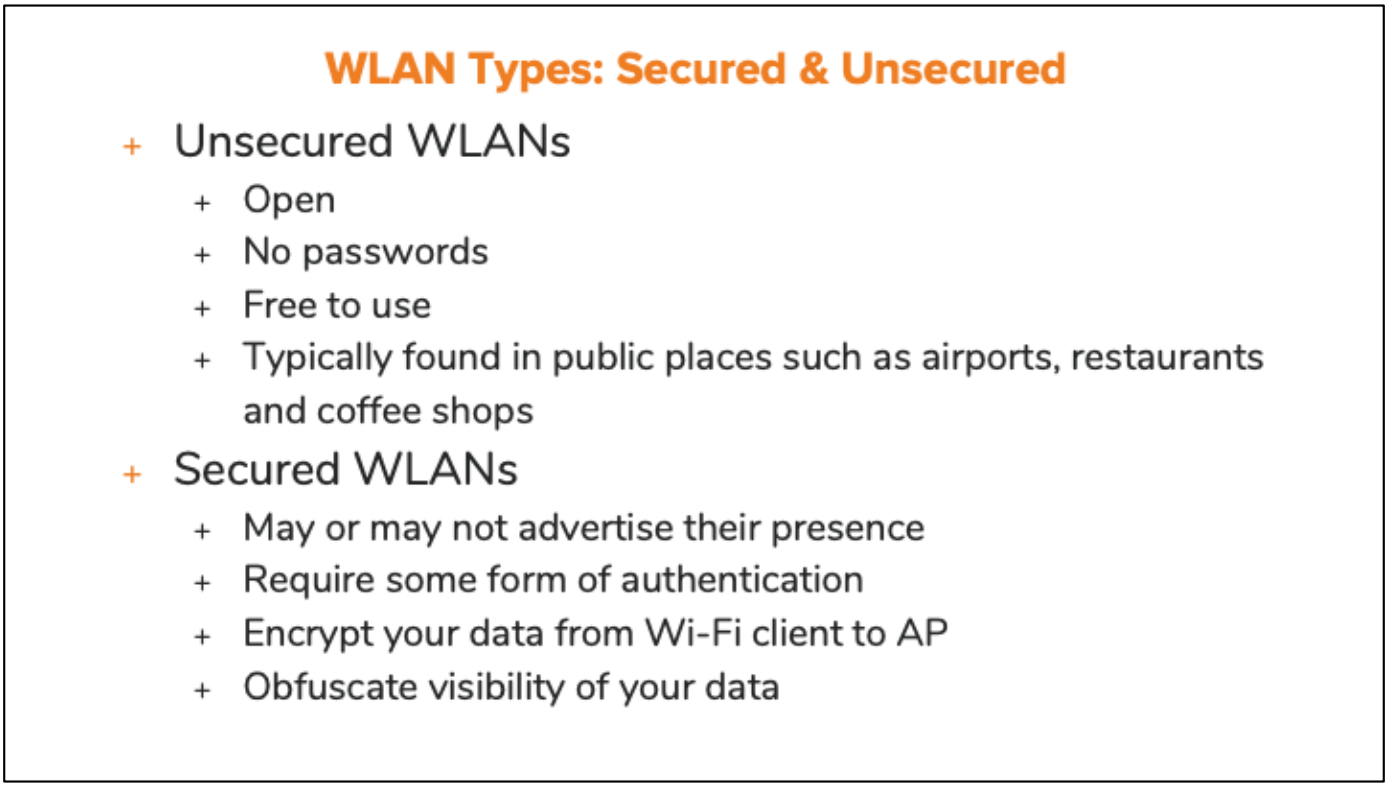
Topic Overview

+ Why we need WLAN security
+ Difference between secured and unsecured WLANs
+ Expectations of WLAN security
+ Components of WLAN security

Why The Need For Security

- WLANs are not the same as wired LANs
- Wired LANs
  - Each host connected to a unique switchport
  - Hosts within same VLAN have no visibility to each other's unicast traffic
  - Devices not physically connected to the switch have no networking capability
- WLANs
  - All hosts share the same medium (the air)
  - Hosts connected to the WLAN can see each other's frames (unicast or not)
  - Any device within proximity of the RF used on the WLAN can see everything on that WLAN

The last bullet is emphasizing that a device doesn't need to actually be formally participating in the WLAN in order to sniff traffic. It's very difficult to control where RF energy goes (as opposed to a physical cable). Any device with an antenna within range of the RF energy can see everything that is being propagated using that RF energy. So devices that are invisible to you (because they haven't formally joined/associated with your WLAN) could very easily be spying on you.



An unsecured WLAN is not necessarily a bad thing as long as you know in advance (before you connect to it) what you're getting into. Keep in mind that many people assume that (even over an unsecured WLAN) their data is safe if they are going to secure websites. However there are still several very popular websites out there that use insecure HTTP (which does not encrypt anything) as opposed to secure websites that utilize HTTPS. When browsing one of these HTTP-based websites over an unsecured WLAN, everything you send and receive is free for anyone else to see.

Whose Perspective Is It?

- The objectives of Wi-Fi security vary depending on the perspective of who needs it
- Network Administrator:
  - Only allow authorized people onto the WLAN
  - Only provide authorized resources via the WLAN
  - Restrict the quantity of WLAN clients
  - Detect rogue access points
- Network User:
  - Keep Wi-Fi data safe via encryption

As you can see, while the Network Administrator might provide encryption as a service to the Wi-Fi user, it may not be the primary concern of the Network Admin (unless they too, are using the same WLAN for their own network access).

When most people think of Wi-Fi they assume that encryption is naturally a part of it. But when connecting to a Guest Wi-Fi network (as an example) there may be no encryption at all. For example, an Open Wi-Fi network that uses a website for authentication (called a Web Portal or Walled Garden) may give you access to the WLAN after providing a password but provide for no encryption after that.

Three Components Of Security

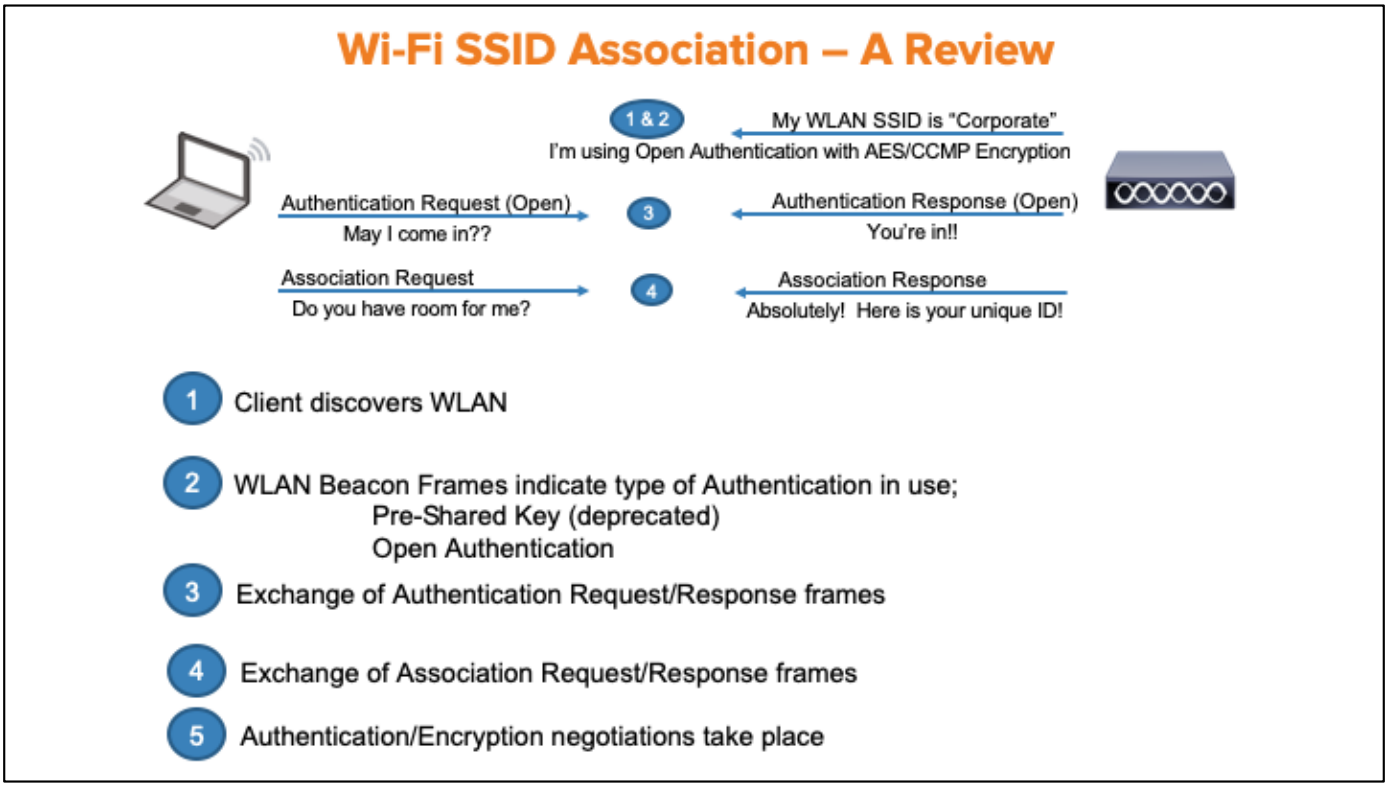
- WLAN Security is composed of three pieces
  - Authentication
  - Data Confidentiality
  - Data Integrity
- All of these are typically accomplished after you've already associated to your SSID
- Authentication can occur independently of encryption/integrity verification
- Encryption and data integrity go together

Thanks for Watching!


Wi-Fi Security: Authentication
ine.com

Topic Overview

+ A review of Wi-Fi SSID association
+ Methods of authentication without encryption
+ Identifying unsecured WLANs



Display WiFi capture in Wireshark. Search for Beacons: wlan.fc.type_subtype == 0x0008
At the end of the Beacon capture, expand the "RSN Capabilities" Information Element and you'll see what kind of Authentication (and Encryption) the access point supports.
http://www.hitchhikersguidetolearning.com/2017/09/17/rsn-information-element/

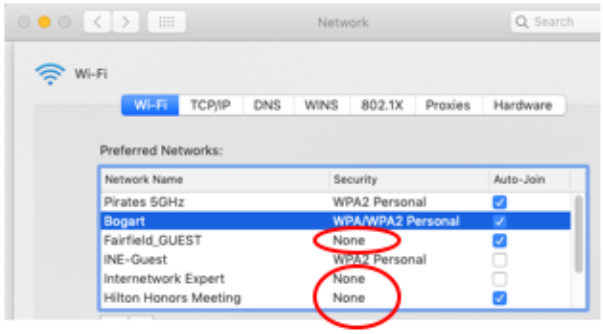
Association: This stage finalizes the security and bit rate options and establishes the data link between the WLAN client and the AP. If a client has joined a network and roams from one AP to another within the network, the association is called a re-association

WLAN Authentication Overview

- Authentication can be accomplished with or without encryption
- Two ways of implementing authentication:
  - Authenticate the user
  - Authenticate the device

Standalone Authentication

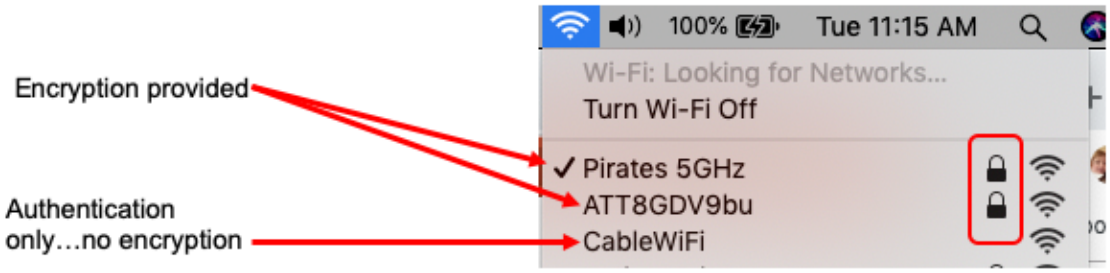
- Methods without encryption:
  - Pre-Shared Key (deprecated)
  - Web Authentication (a.k.a. Captive Portal)
  - 802.1x
  - MAC Authentication



"Security" in the context of this screenshot means, "Did the beacons captured for this network indicate any ability to encrypt traffic?"

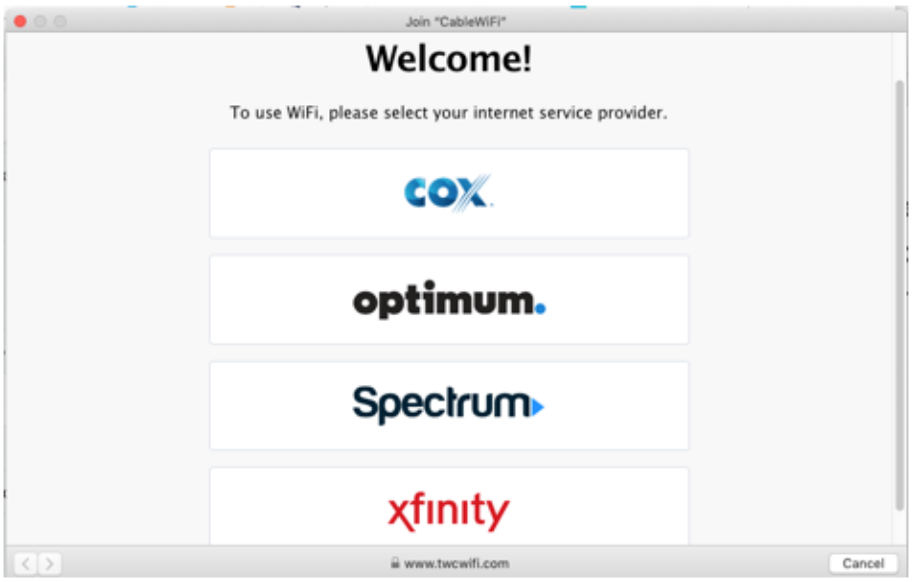
Identifying Unsecured Wi-Fi Networks

- When a Wi-Fi network displays as "Secured" this means the AP has advertised a requirement to use encryption
- Unsecured Wi-Fi does not provide data confidentiality
  - May or may not require authentication
  - Authentication typically provided via a Captive Portal



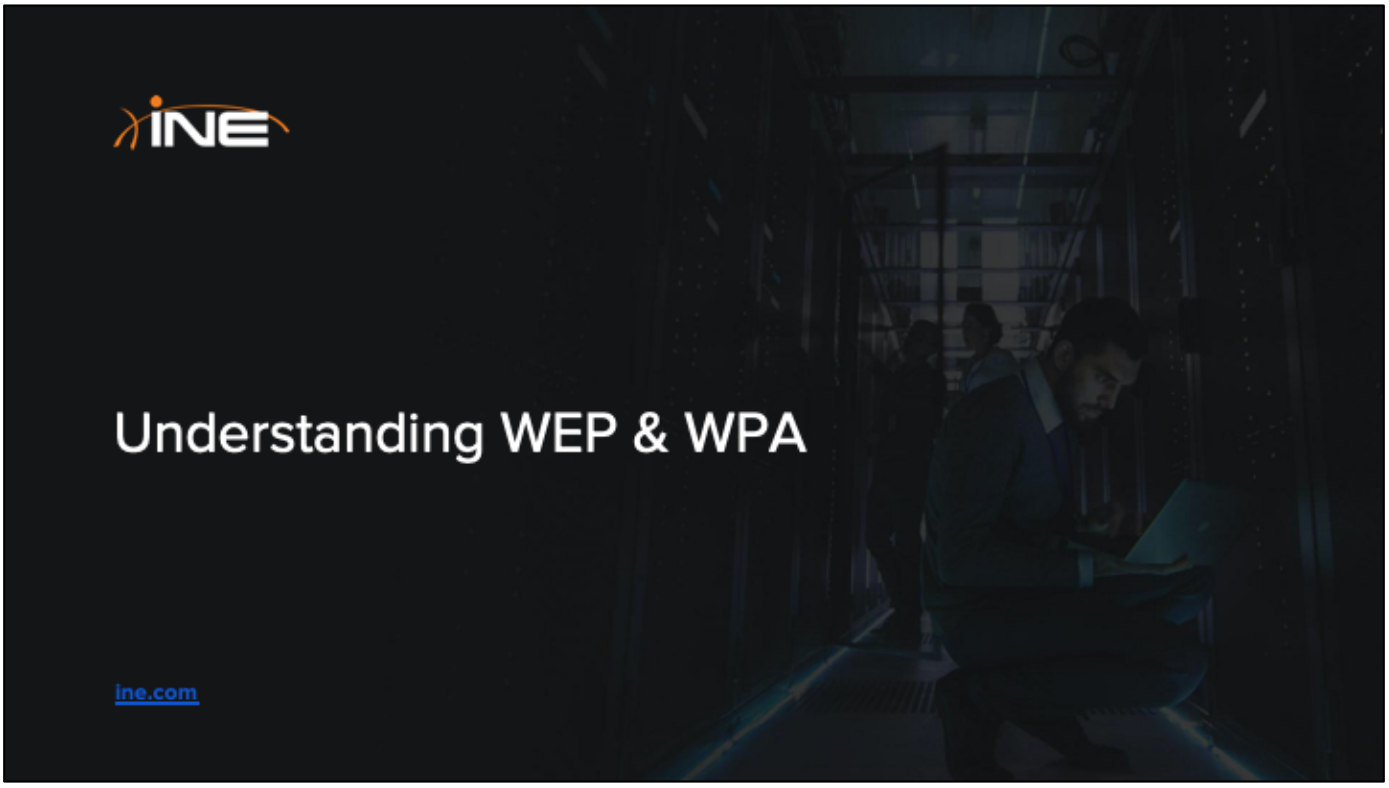
Note that from the access point's perspective, encryption is not optional. If the AP advertises that it CAN do encryption, this means the client MUST support it…or find another WLAN to connect to.

Identifying Unsecured Wi-Fi Networks



In the previous graphic we saw that the “CableWiFi” SSID was unsecured. When selecting that network, we are still prompted to input some kind of credentials for the sake of Authentication…but our data will not be encrypted and is not safe.

Thanks for Watching!

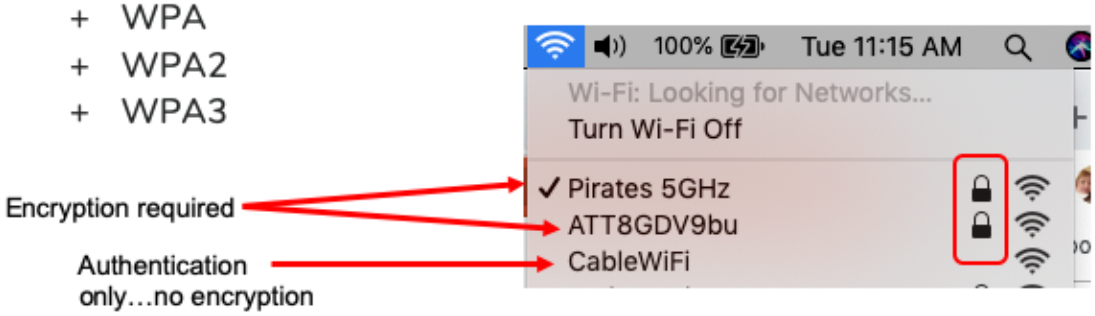

Understanding WEP & WPA
ine.com

Topic Overview

+ Identifying encrypted WLANs
+ Where encryption takes place
+ An overview of WEP vs WPA
+ Timeline of Wi-Fi security
+ WEP
+ WPA Personal & Enterprise

Identifying Encrypted Wi-Fi Networks

- When a Wi-Fi network displays as "Secured" this means the AP has advertised a requirement to use encryption
- Wi-Fi algorithms/protocols that provide encryption also provide for data integrity:
  - WEP
  - WPA
  - WPA2
  - WPA3



Note that from the access point's perspective, encryption is not optional. If the AP advertises that it CAN do encryption, this means the client MUST support it…or find another WLAN to connect to.

Where Encryption Takes Place

- Only the Wi-Fi data (i.e. Frame Body) gets encrypted
- The access point can be enabled to advertise various encryption standards and protocols
- Encryption and decryption happen between access point and Wi-Fi client
  - Only Data frames encrypted, not Management frames

WPA2 introduced an optional feature (also supported in WPA3) called MFP or Management Frame Protection. This serves to encrypt, or at least prevent the forging of, certain Management frames. However this feature only works on a very small subset of the Management Frames in Wi-Fi…namely the frametypes of Deassociation, Deauthentication and QoS Action frames. Many clients don't support this feature so it isn't widely used.

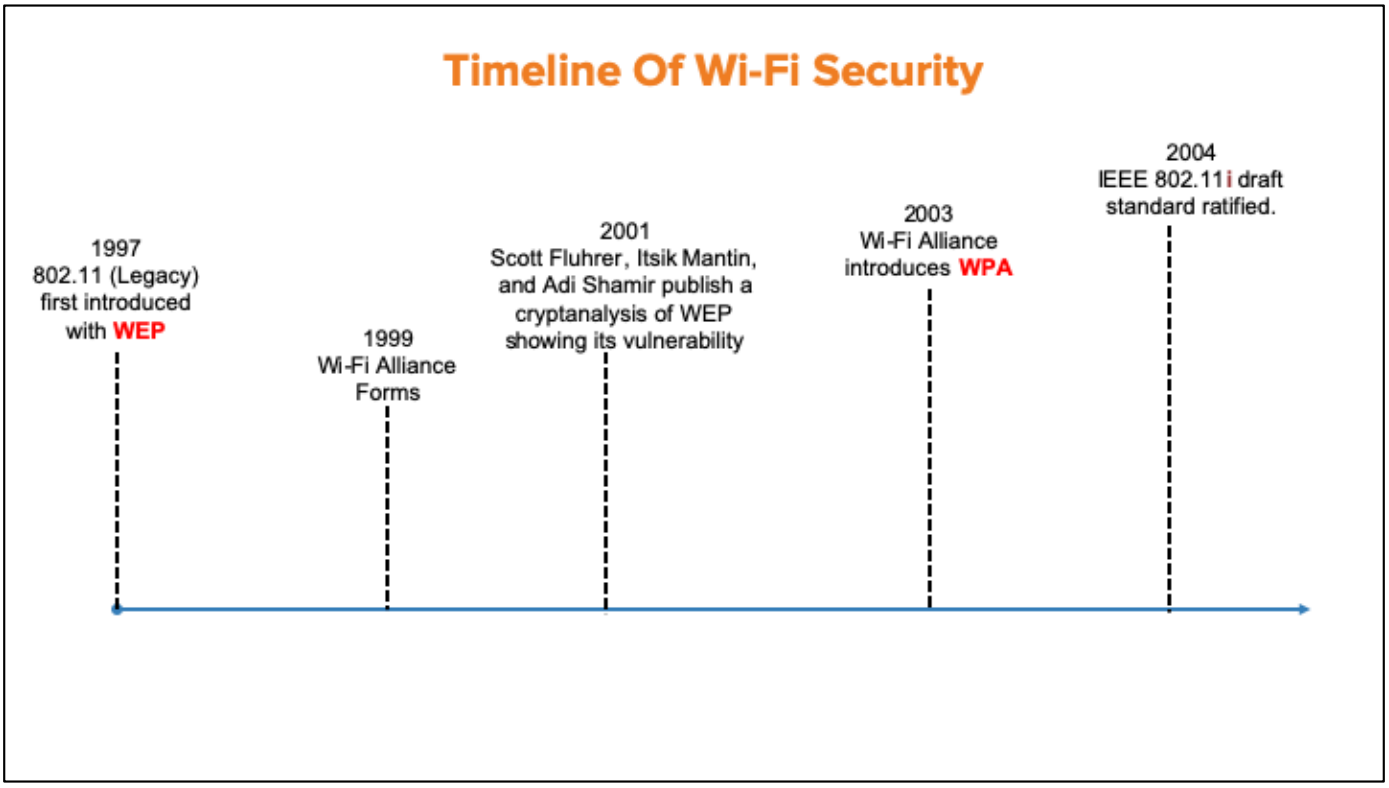
WEP vs WPA

- WEP
  - Wired Equivalent Privacy
  - Early form of Wi-Fi security written into original 802.11-1997 standard
  - Utilized RC4 Encryption Cipher
  - Considered unsafe and is now deprecated
- WPA = Wi-Fi Protected Access
  - Introduced by Wi-Fi Alliance to fix Wi-Fi security problems found in WEP
  - WPA was based on a draft of IEEE 802.11i amendment
  - WPA was intended to be an intermediate measure until the full 802.11i amendment was ratified

The main problem with WEP was twofold:
---WEP provided the same Security Key (i.e. Password) to everyone who wanted to join the WLAN.
---This static key was used for both Authentication as well as for Encryption of data.

WEP was officially retired by the Wi-Fi Alliance in 2004.

To better understand WPA, WPA2 and WPA3 it helps to start by viewing them in the context of history (what preceded them, and when they came out). Let's look at the next slide.



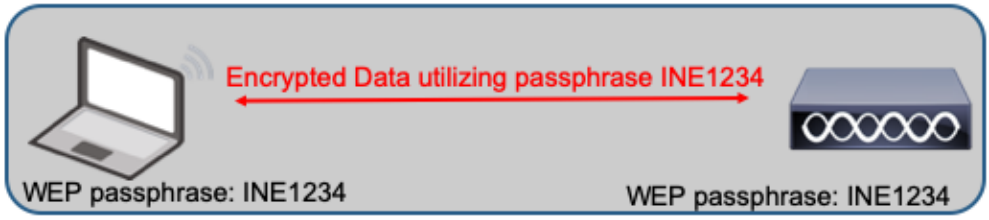
The original 802.11-1997 standard had a section for Authentication and privacy. Two forms of Authentication were provided for:
----Open System (no authentication at all)
----Shared Key (in which a Wi-Fi client provided a shared-key/passphrase with the AP during the exchange of Authentication Management frames).

The 802.11-1997 standard only provided for WEP as an Encryption/Privacy protocol…which was soon thereafter proven to be crackable.

The Wi-Fi Alliance was/is a trade association tasked with tested vendor products to ensure they are interoperable and conform to 802.11 standards. When they DO, vendors can apply a Wi-Fi Alliance logo to their product.

2003: The Wi-Fi alliance got a hold of a draft form of 802.11i. That draft specified improvement to Wi-Fi security using stronger protocols and methods than had previously been in the original 802.11-1997 standard. Rather than wait (who knows how long) for 802.11i to be formally ratified by the IEEE, the Wi-Fi Alliance put together their own recommendations of how Wi-Fi security should be implemented (based on the draft of 802.11i) and they called it WPA (Wi-Fi Protected Access).

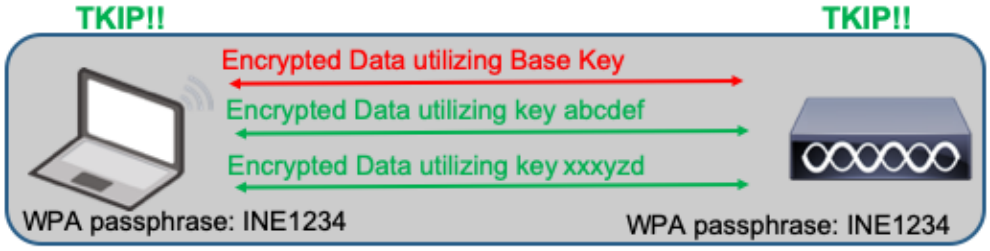
WEP



- Static (unchanging) passphrase
  - 64-bit, 128-bit or 256-bit
  - 128-bit most common
- Data is encrypted to/from access point
  - Utilized RC4 encryption cipher
  - Easily cracked with a static passphrase

Even though WEP has been deprecated for over a decade, it helps to understand the basics of WEP so that you can appreciate the motivation behind WPA, and why WPA is different than WPA2.

WPA Personal



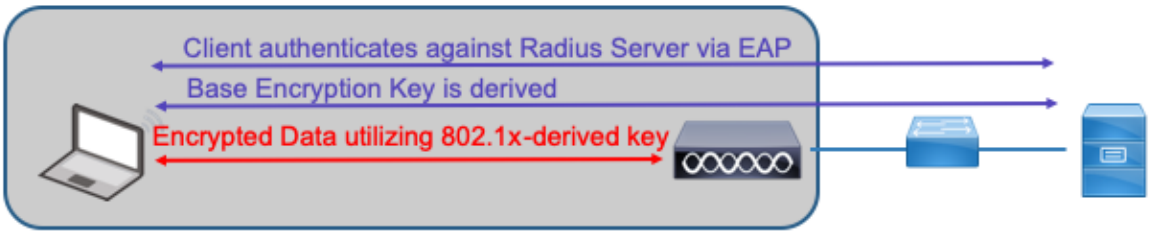
- Initial passphrase set for Authentication
- WPA Base Key derived for encryption of data
  - Up to 256-bits
  - Derived from the static passphrase (plus other elements)
- Data is encrypted to/from access point
  - Utilized RC4 + TKIP encryption cipher
  - Message Integrity Check (MIC) added
  - TKIP provided a per-packet key system

Due to WEP's vulnerabilities, WPA was introduced by the Wi-Fi Alliances in 2003.

Among WPAs new security features was MIC (Message Integrity Check) which was a way to determine if an attacker had captured or altered packets passed between the access point and client.

You might ask, "with a system that changed the encryption key per-packet…how was WPA insecure??" Without going too much into the weeds, the problem with WPA Personal was that the various keys that were derived dynamically for per-packet encryption were all derived from a well-known value, the Passphrase. If the Passphrase were something easily guessable (or crackable with a dictionary attack) then it would be fairly easy to derive the keys and start decrypting everyone's traffic.

WPA Enterprise



- Client utilizes 802.1x to authenticate against Radius Server
- 802.1x exchange provides initial encryption key
  - Encrypted exchange of data between client and AP begins
- Encryption of data done by RC4 + TKIP (per-packet key rotation)

Whenever you see the word “Enterprise” in the context of WPA or WPA2 think “802.1x with an Authentication Server”.

Depending on the document you read, it can be confusing if WPA supported only TKIP…or both TKIP and AES (Advanced Encryption Standard). It would seem that history, once again, can answer this question. WPA was designed so that older devices that had previously used WEP could (with a simple firmware upgrade) now support WPA. Well, a firmware upgrade was not enough at that time to support the more robust AES protocol. So initial implementations of WPA ONLY supported TKIP (which COULD be accomplished with a firmware upgrade as it was simply an enhancement to RC4, which WEP was already using).

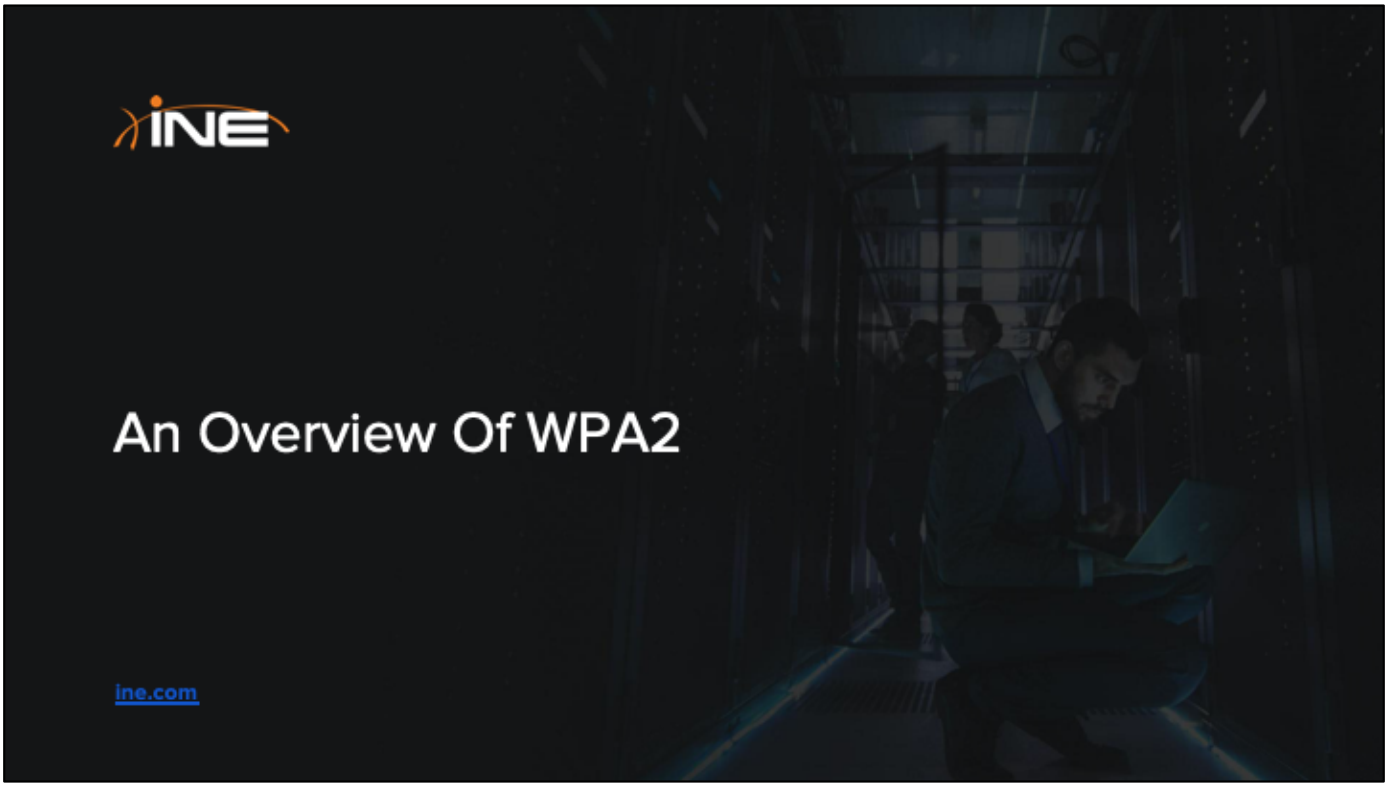
As time passed, and more and more devices were capable of both AES and TKIP, vendors started introducing WPA with both options, but this wasn’t the way it was from the beginning.

When WPA started supporting both cipher suites (TKIP and/or AES) WPA Enterprise strongly encouraged the use of AES but provided TKIP for backwards compatibility with Wi-Fi clients that didn’t support AES.

The real strength behind an Enterprise version of WPA (or WPA2) is that there isn’t a single, value (like a common Passphrase) that is known by everyone and is also used as an ingredient in creating the Base Encryption Key (whether you’re doing

AES or TKIP). Instead once a user authenticates with their own, personal credentials, everything for creating the Base Key is dynamically derived by the 802.1x Authentication Server on a per-user, per-session basis. Additionally, EAP can periodically change the Base Key while a session is still in-use by a Client.

Thanks for Watching!

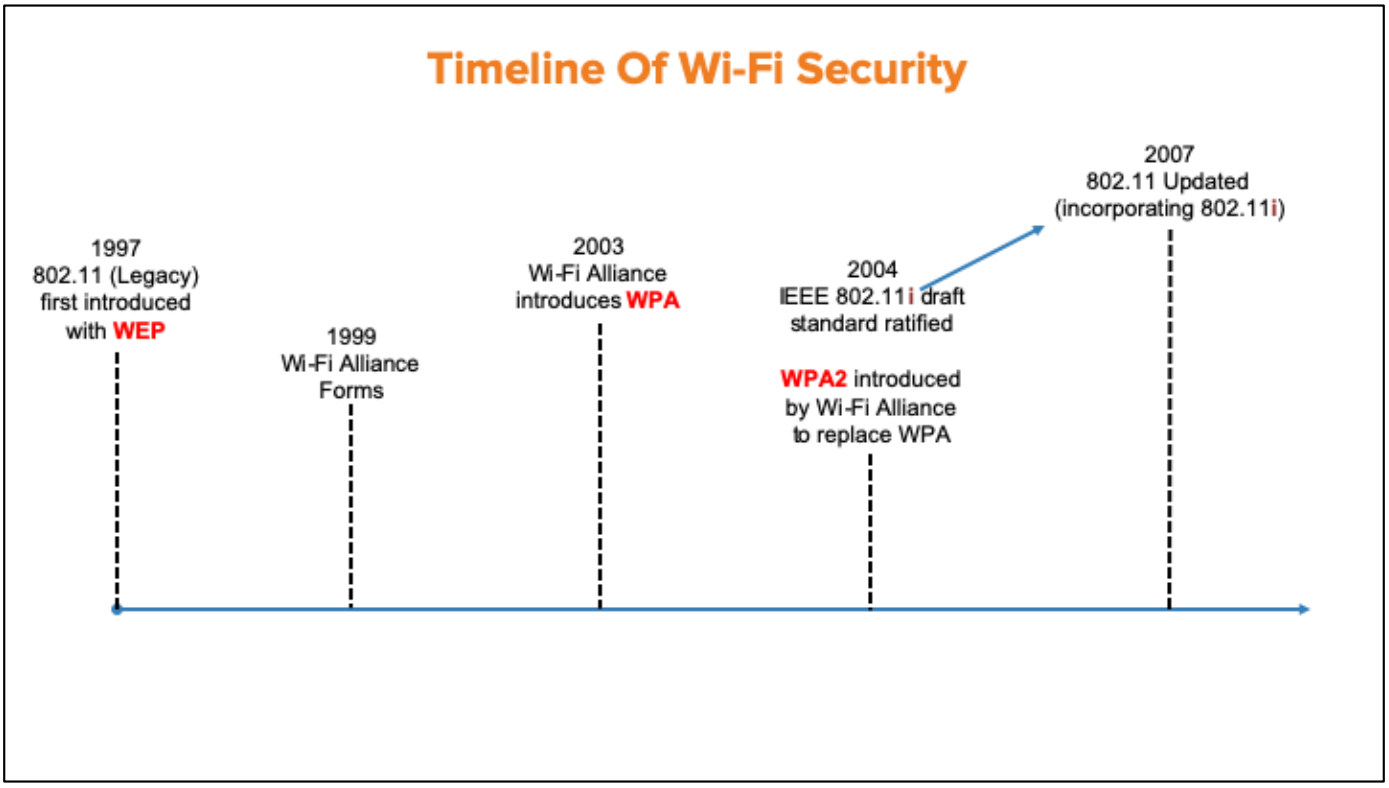

An Overview Of WPA2
ine.com

Topic Overview

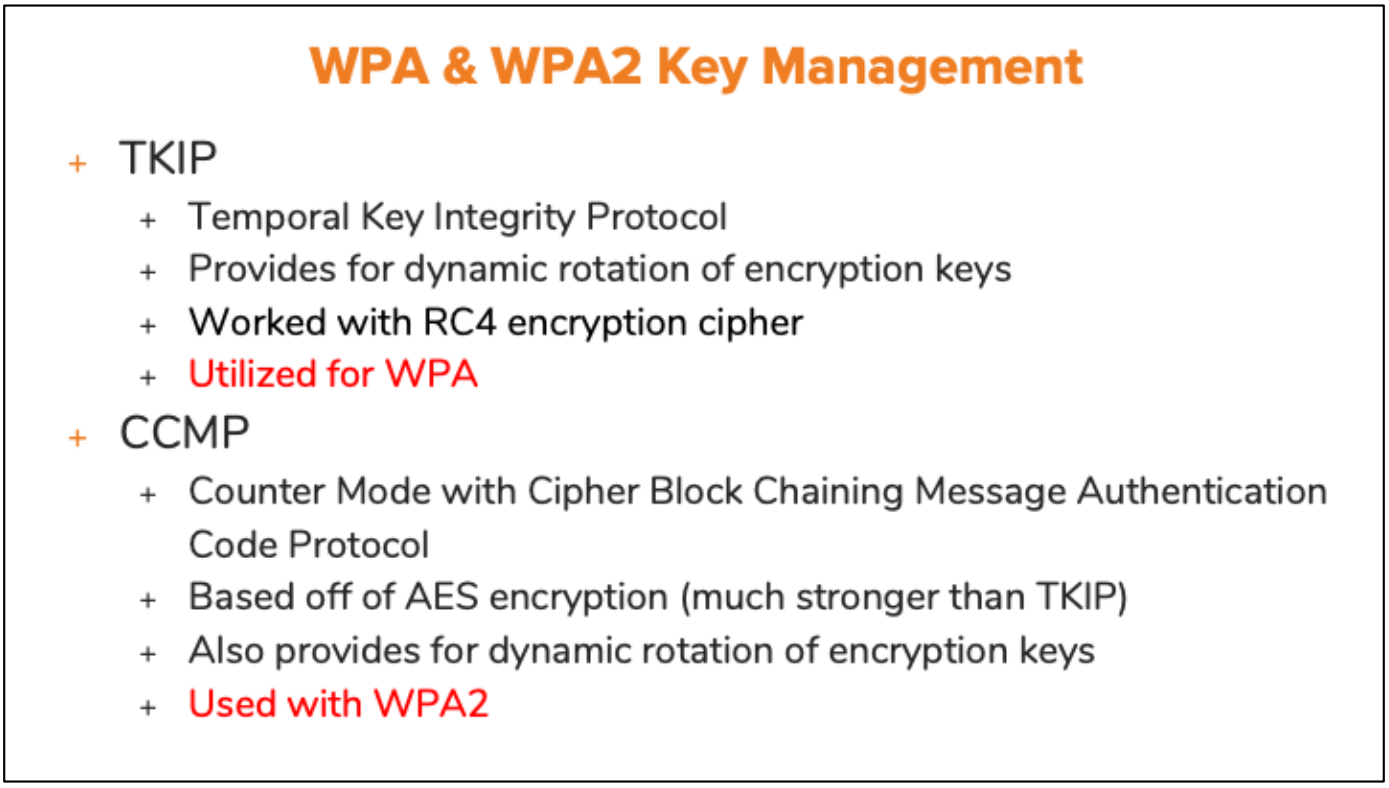
+ The downside of WPA
+ Timeline of Wi-Fi security
+ WPA & WPA2 key management
+ WPA2 Personal & Enterprise
+ WPA & WPA2 summary

The Downside Of WPA

- WPA initially only supported TKIP
- Once 802.11i was formally ratified, it became clear that all of the standard's components provided stronger security than WPA
- WPA2 was created to be fully-compliant with 802.11i security standards including:
  - Included the mandatory use of AES-CCMP encryption for WPA2 Enterprise (RC4 and TKIP no longer an option)
  - 802.1x could be used in Ad Hoc mode (rarely used)
  - Options for speeding 802.1X re-authentication were added



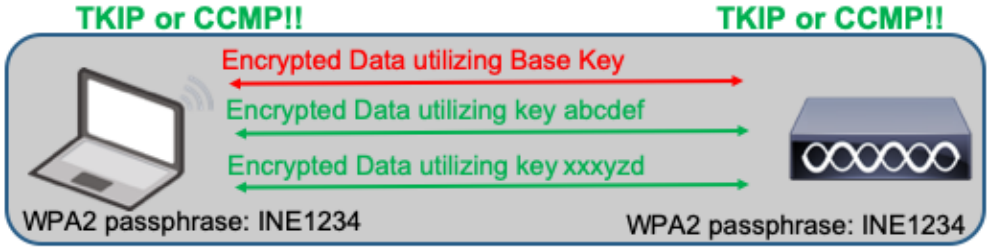
2007: 802.11 was updated which now formally incorporated all previous clauses and amendments, including the Security enhancements that had previously been introduced with the 802.11i amendment.



WPA and WPA2 utilize ”Symmetric Key Cryptography”, which means that both sides use the same key (think, passphrase) in order to encrypt and decrypt messages. When using WPA/WPA2 Personal Edition, everyone has the same Pre-Shared key. You might think, “how does this protect me if my neighbor is using the same key that I am”? The Pre-Shared key IS used for Authentication, however it is only one element (among many) used to come up with your Symmetric Encryption Key. So even though you and your neighbor have the same Pre-Shared key, the algorithms used by WPA and WPA2 will use this key, but still ensure you both end up with unique encryption keys. However, it is risky to have everyone’s Encryption Key start from the same source (a shared, well-known passphrase).

TKIP was one of the (many) improvements that WPA made over WEP, providing the ability to have your encryption key rotate (or change) with each packet to prevent hackers from guessing what it was.

WPA2 Personal

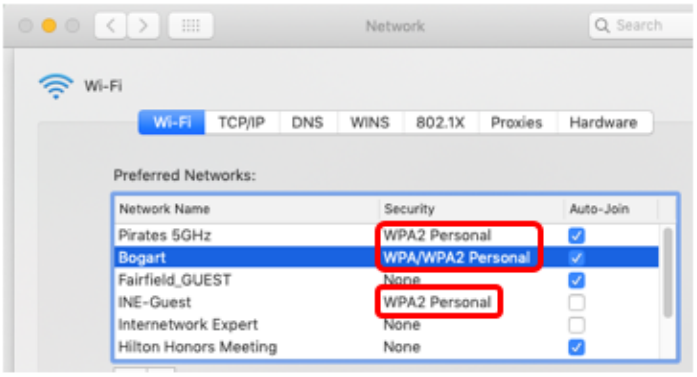


- Initial passphrase set for Authentication
- WPA2 Base Key derived for encryption of data
  - Up to 256-bits
  - Derived from the static passphrase (plus other elements)
- Data is encrypted to/from access point
  - Utilized RC4 + TKIP or...
  - CCMP-AES encryption ciphers (recommended)

When selecting RC4 + TKIP, WPA Personal and WPA2 Personal aren't much different if you're only thinking about encryption and authentication. The real power of WPA2 Personal is when CCMP-AES encryption is selected (something that wasn't available for WPA Personal).

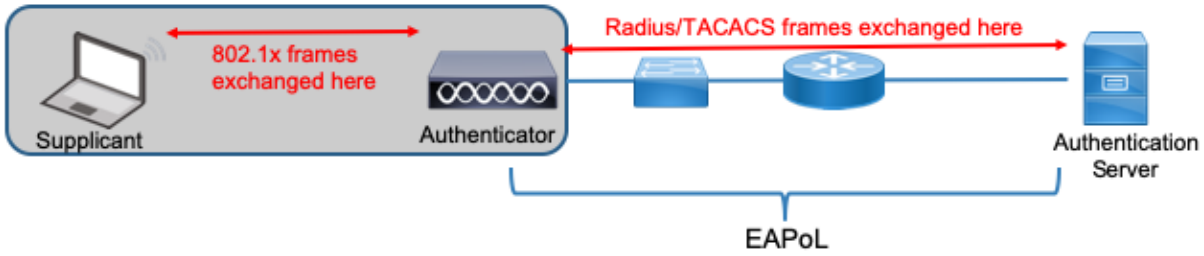
Identifying WPA & WPA2 Personal

- WPA/WPA2 Personal mandates the use of a Pre-Shared Key for authentication

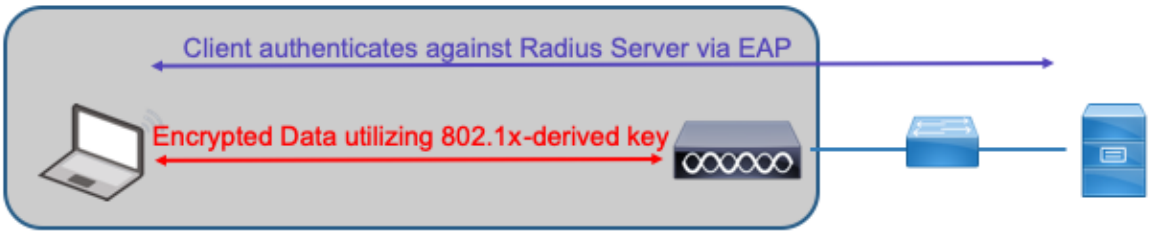


WPA & WPA2 Enterprise

- WPA/WPA2 Enterprise mandates the use of an 802.1x infrastructure for authentication



WPA2 Enterprise



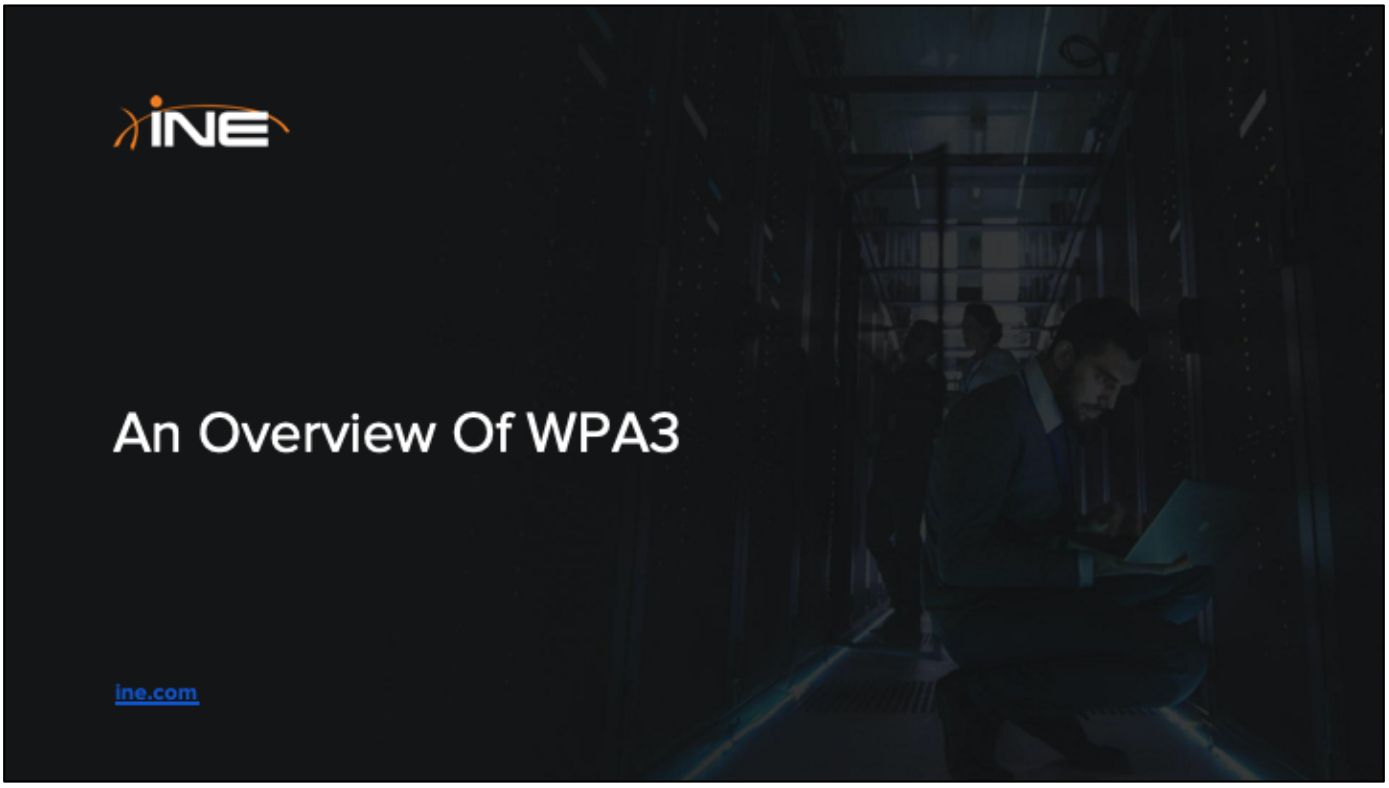
- Client utilizes 802.1x to authenticate against Radius Server
- 802.1x exchange provides initial encryption key
  - Encrypted exchange of data between client and AP begins
- Encryption of data must be done by CCMP-AES (per-packet key rotation)

Remember, that because WPA2 was the full implementation of the 802.11i standard, it contained a lot of additional features above-and-beyond authentication and encryption methods.

WPA & WPA2 Summary

- WPA = Draft version of 802.11i
- WPA2 = Fully compliant with 802.11i clause
- Both offer “Personal” and “Enterprise” editions
  - Personal Edition meant for SOHO use
  - Enterprise Edition meant for larger-scale Wi-Fi deployments
- Many companies use WPA/WPA2 Personal (instead of Enterprise) due to easier implementation

Thanks for Watching!


An Overview Of WPA3
ine.com

Topic Overview

+ Why did we need another WPA?
+ Introduction to WPA3
+ Timeline of Wi-Fi security
+ WPA3 Personal
+ WPA3 Enterprise
+ Other WPA3 enhancements

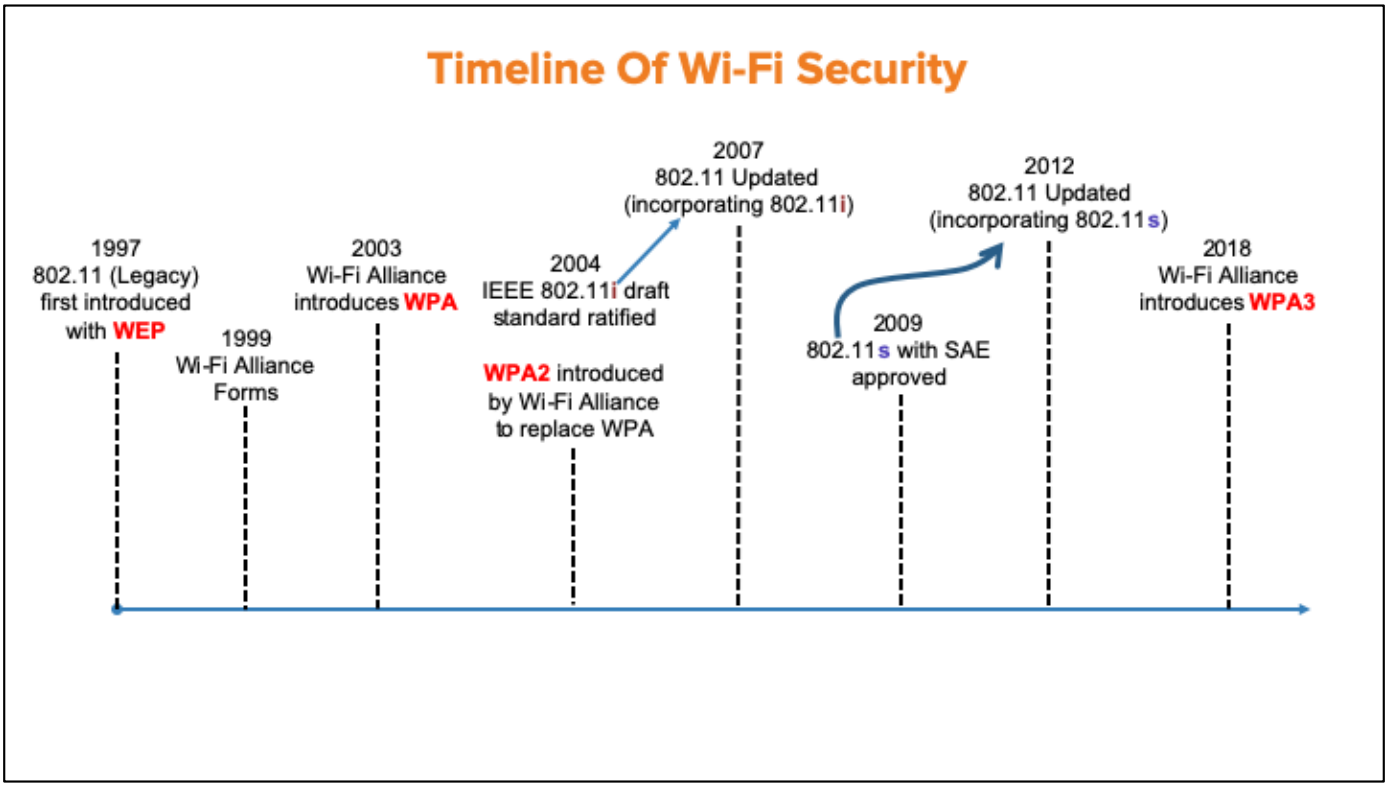
Why Did We Need Another WPA?

- Since WPA2 was introduced in 2004 the landscape for Wi-Fi has significantly changed:
  - Users are more mobile, quickly bouncing from one wireless network to another
  - IoT devices which don't have a GUI or CLI
  - People want Wi-Fi encryption, even over Open networks (think Airports and Restaurants)

Introduction To WPA3

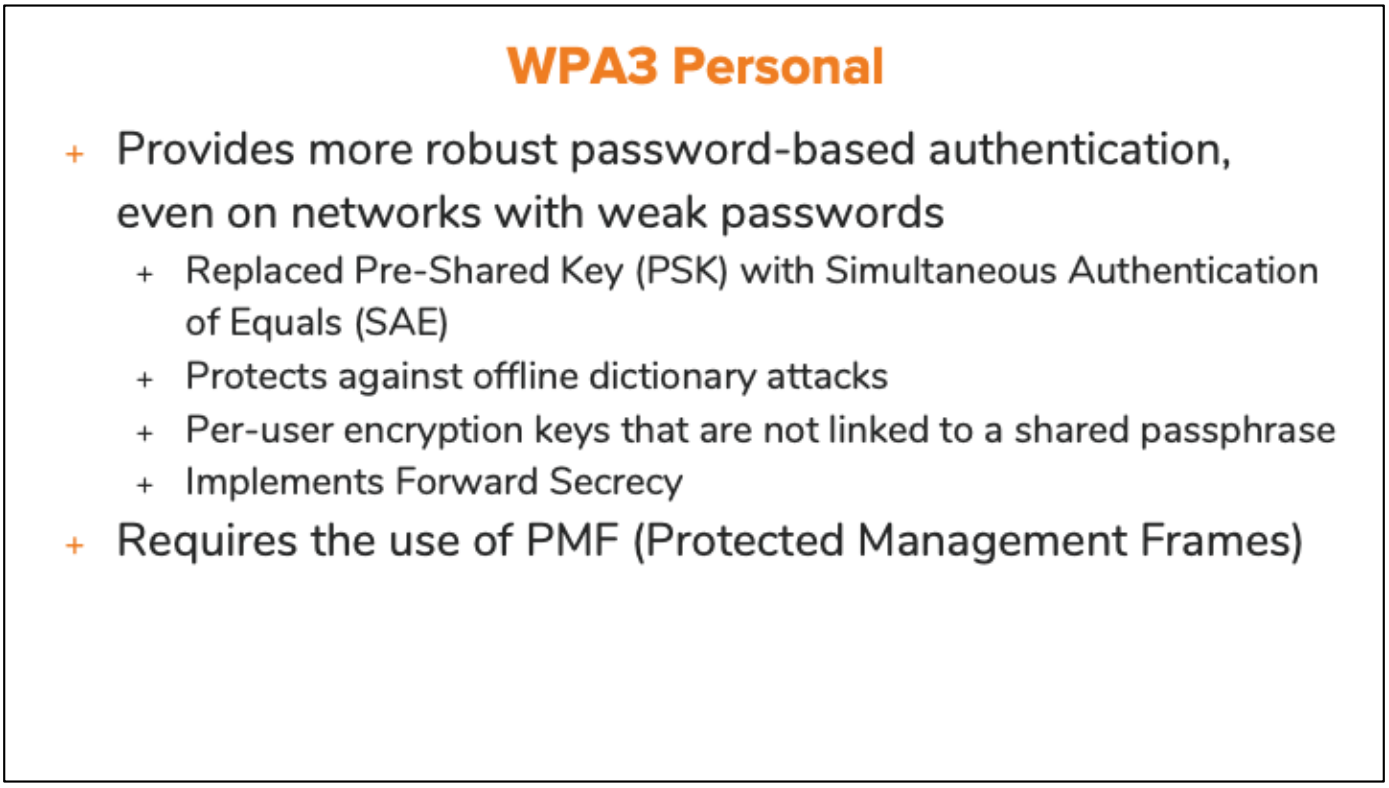
- Adds several new features to WPA
- Still retains concept of WPA Personal and Enterprise
- Different features available in Personal vs Enterprise

WPA3 was announced January 8th, 2018 by Wi-Fi Alliance



2007: 802.11 was updated which now formally incorporated all previous clauses and amendments, including the Security enhancements that had previously been introduced with the 802.11i amendment.

2009: 802.11s was primarily concerned with introducing a new form of Wi-Fi called Mesh Routing. However, in that amendment, a new form of Security was introduced (for access points to be able to authenticate with each other) called SAE (Simultaneous Authentication of Equals). This new (and better) form of authentication would then be incorporated a few years later into WPA3.



WPA2 upgraded the security of WPA by introducing a 4-way handshake between Client and AP. However, the nature of this handshake became susceptible to the KRACK attack (Key Reinstallation Attack) in which a Man-in-the-Middle could eventually discover the WPA2 derived encryption key.

WPA3 defines a new handshake (called, SAE) that "will deliver robust protections even when users choose passwords that fall short of typical complexity recommendations". In other words, even if you're using a weak password, the WPA3 standard will protect against brute-force attacks where a client attempts to guess at passwords over and over until they find the correct one.

Forward Secrecy simply means that even if someone were to capture (in plain text) the entire WPA2/WPA3 handshake, they would not be able to derive the encryption key that was used to encrypt to remainder of the Wi-Fi session. Clearly, a device that is susceptible to the KRACK attack would NOT be considered to have Forward Secrecy.

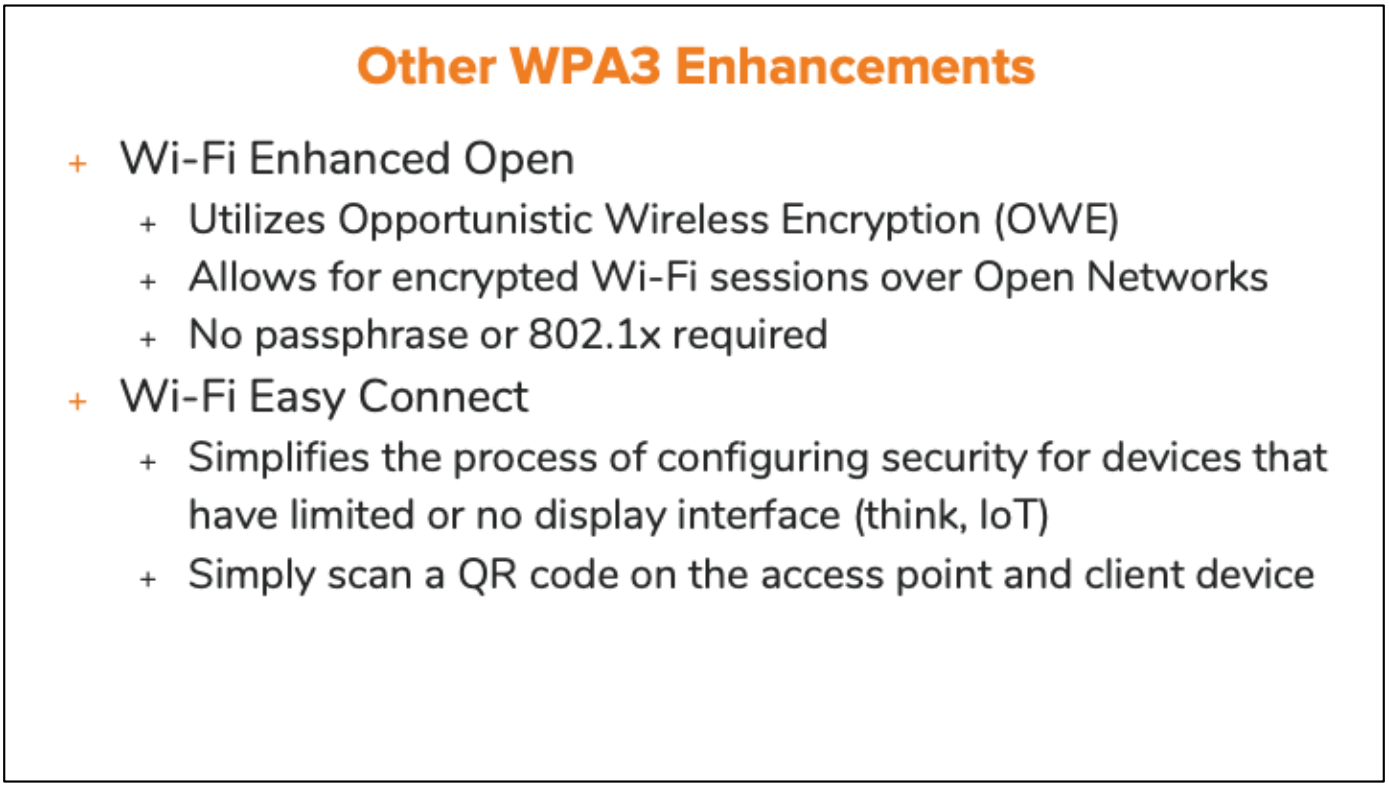
PMF encrypts certain Wi-Fi Management Frames (such as Deauthentication and Deassociation frames) so that someone can't spoof you can kick you off of the network. PMF must be negotiated for all WPA3 connections providing an additional layer of protection from deauthentication and disassociation attacks. This was optional in WPA2 but mandatory in WPA3.

WPA3 Enterprise

- Requires the use of PMF (Protected Management Frames)
- Introduces a new 192-bit-minimum cryptographic security suite "aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite, commonly in place in high-security Wi-Fi networks in government, defense, finance and industrial verticals." – quote courtesy of Wi-Fi Alliance

192-bit security suite, aligned with the Commercial National Security Algorithm (CNSA) Suite from the Committee on National Security Systems. The Committee on National Security Systems (CNSS) is part of the US National Security Agency so this enhanced security is primarily for government, defense, and industrial applications.

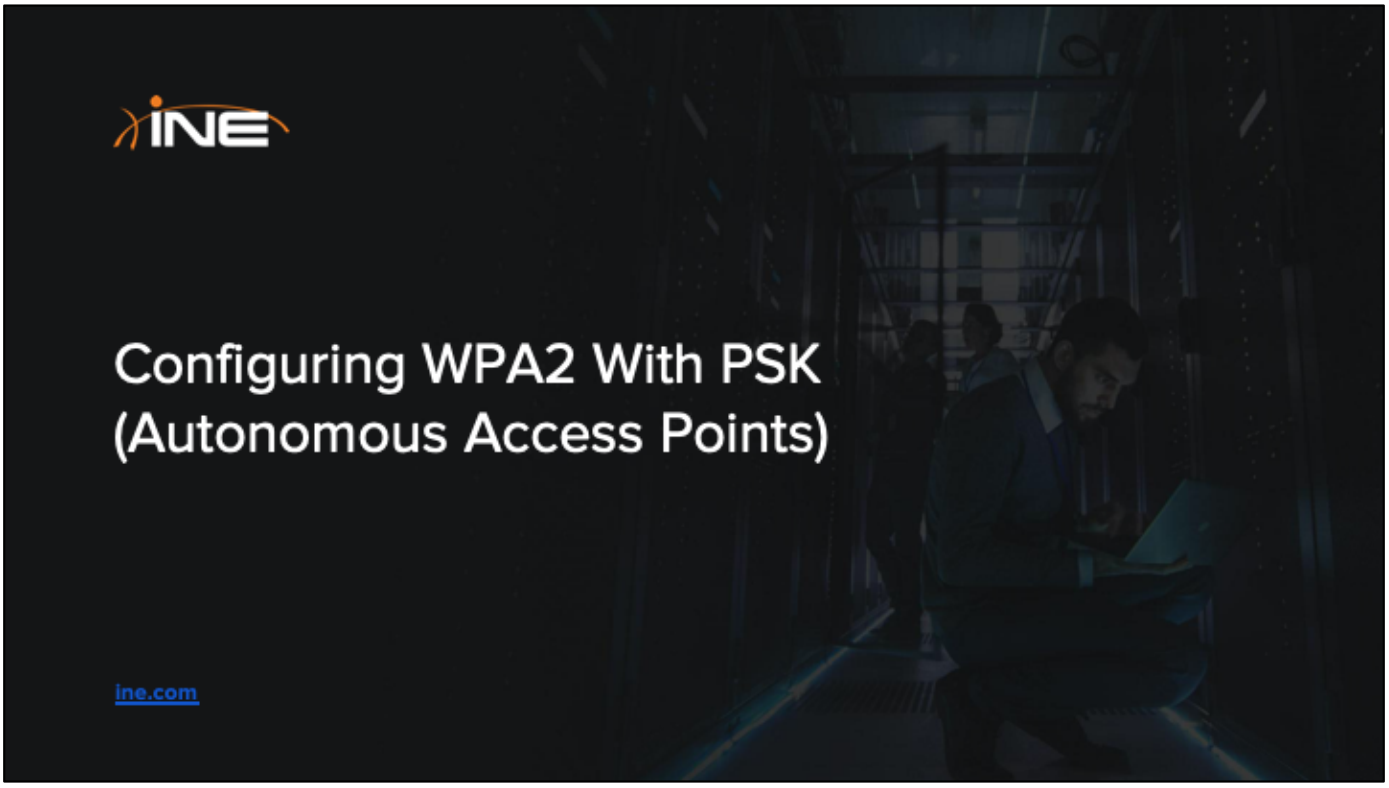
Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve
Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)



Wi-Fi Enhanced Open is actually not a part of the official WPA3 specification but will probably be added into products at the same time they are manufactured to support WPA3 (it is optional for vendors to support it). So in the future, when connecting to an Open network (like in an airport or restaurant) that doesn't have a passphrase, your Wi-Fi client might be required to support Enhanced Open…or it might still be an Open/unencrypted session.

If you're like me and you've wondered, "How can a Wi-Fi Client and access point create an encrypted session between themselves, when there isn't any Pre-Shared Key or anything?" then I encourage you to poke around in RFC 8110 and watch this YouTube Video: https://www.youtube.com/watch?v=E2r5QkgQpUM

Thanks for Watching!


Configuring WPA2 With PSK
(Autonomous Access Points)
ine.com

Topic Overview

+ WPA2 PSK configuration on an autonomous access point

WPA2 Configuration: Autonomous Or Controller?

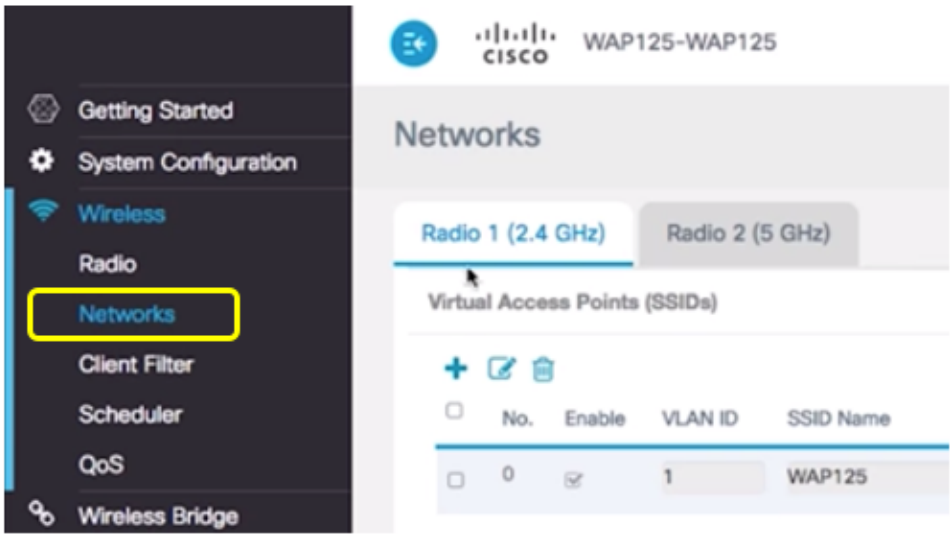
- WLANs can be created/configured in one-of-two ways:
  - On standalone/autonomous access points
  - Via wireless controllers
- Let's see how we'd configure WPA2 with Pre-Shared Key on an autonomous access point...

WPA2 Configuration: Autonomous AP

Step-1: Login to the AP's GUI

WPA2 Configuration: Autonomous AP

Step-2: Find the SSID for which you want to apply WPA2 security.

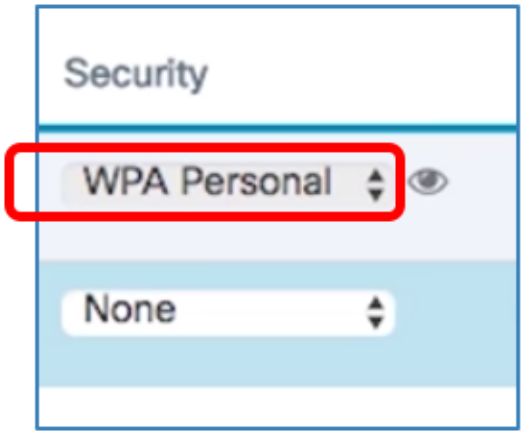


In this particular GUI you would select the “Networks” option. However the GUI for every AP is different but it shouldn’t be too difficult to locate this section in your own APs GUI.

WPA2 Configuration: Autonomous AP

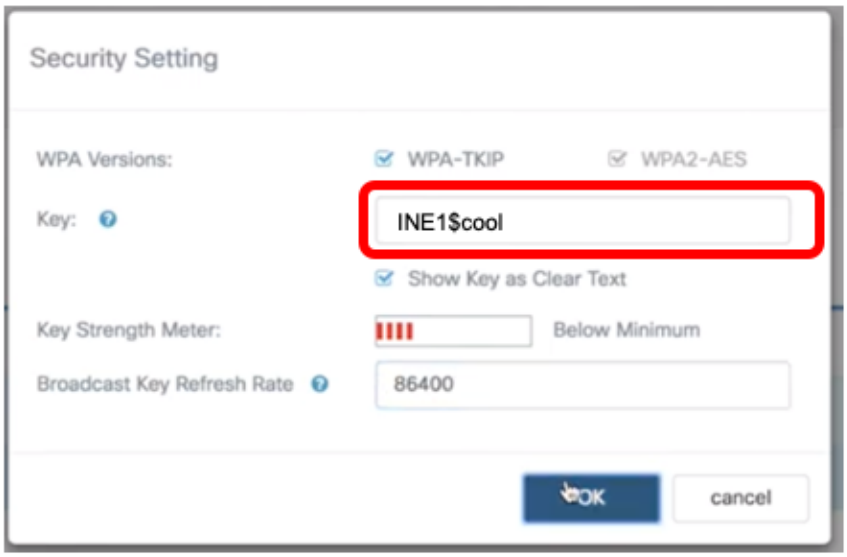
Step-3: Locate the “Security” or “Encryption” section and select WPA2 Personal.

This might display as:
WPA2 PSK
WPA2 Pre-Share



WPA2 Configuration: Autonomous AP

Step-4: Select the WPA2 encryption method and passphrase (i.e. pre-shared key).



In this image we're giving WPA2 the ability to encrypt either via TKIP or AES. However TKIP is insecure and these days, pretty much every device supports AES so you should ideally only check that option.

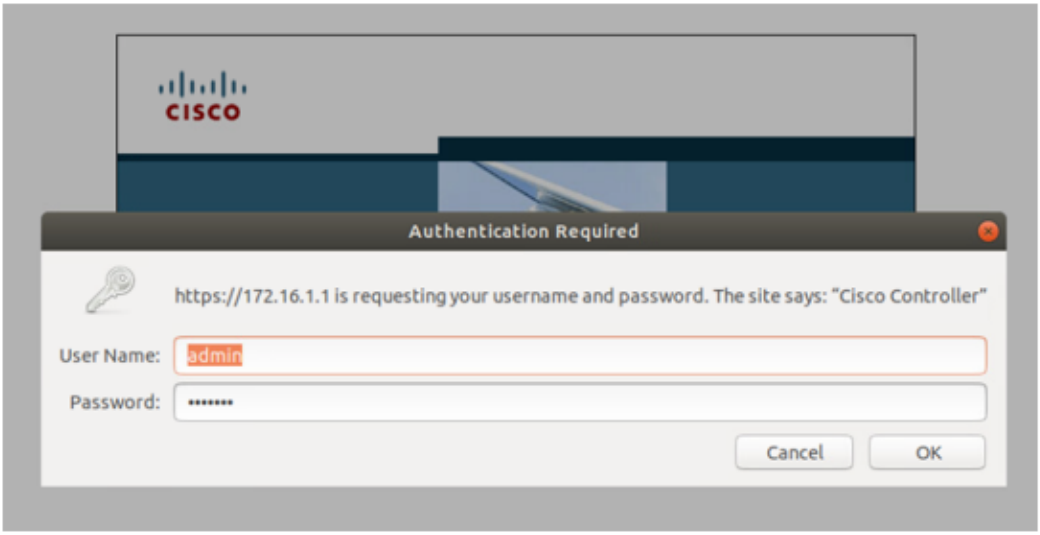
Thanks for Watching!


Configuring WPA2 With PSK
(Wireless Controller)
ine.com

Topic Overview

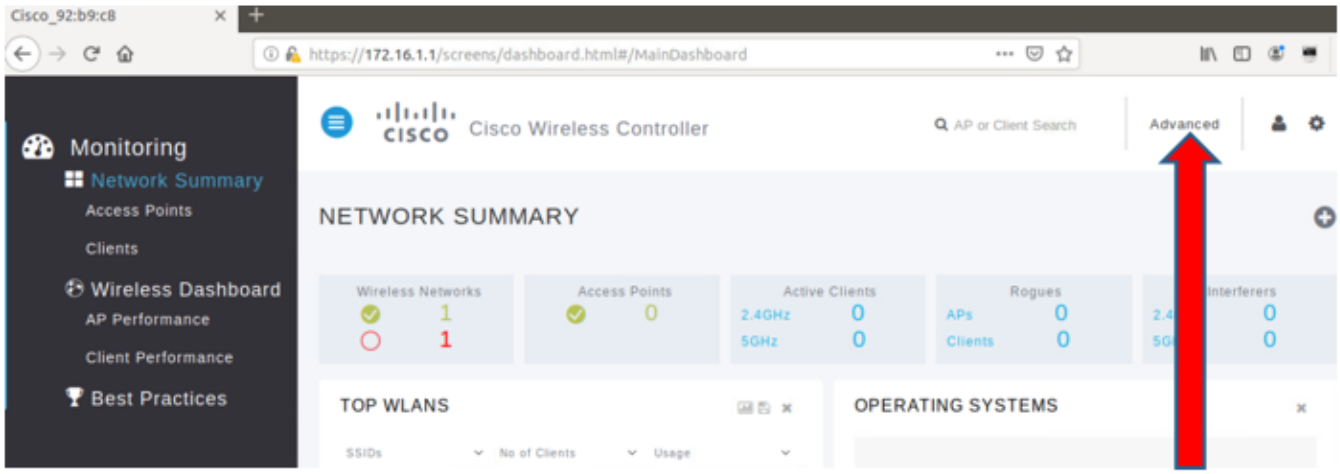
+ WPA2 PSK configuration on a WLAN Controller

WPA2 PSK Configuration: WLAN Controllers



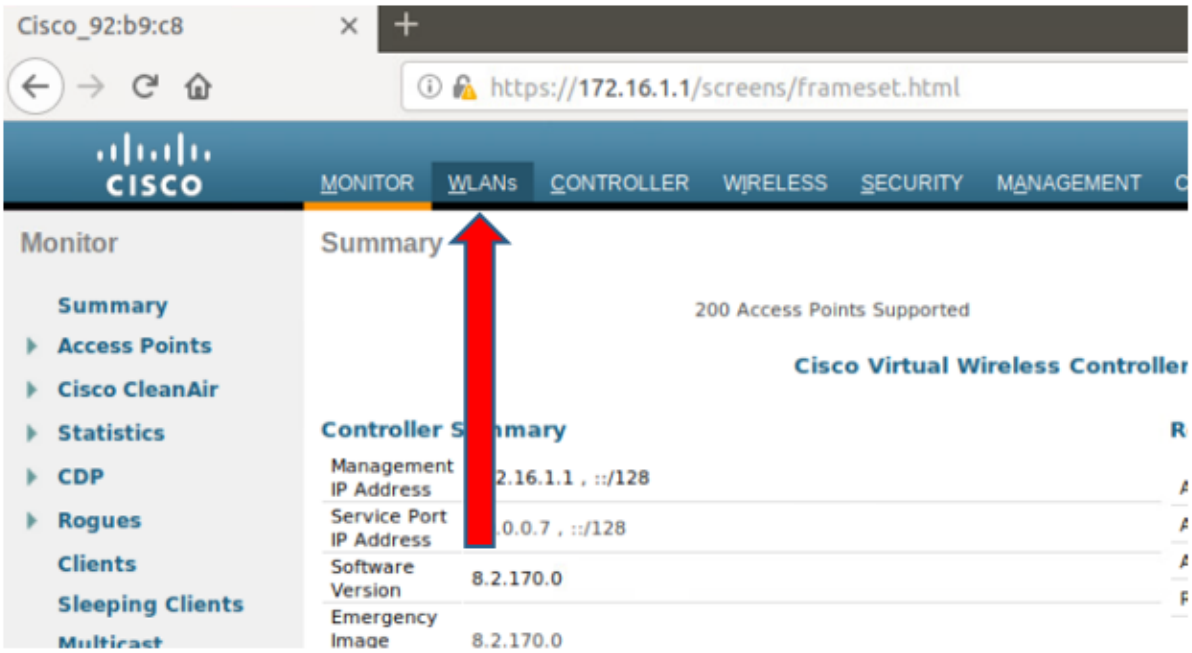
Step-1: Login to the WLAN Controller's GUI

WPA2 PSK Configuration: WLAN Controllers



Step-2: Navigate to the appropriate link or tab which will allow you to configure the Controller (if not already there by default)

WPA2 PSK Configuration: WLAN Controllers



Within the configuration section, select the link, tab or button that will allow you to view all configured WLANs.

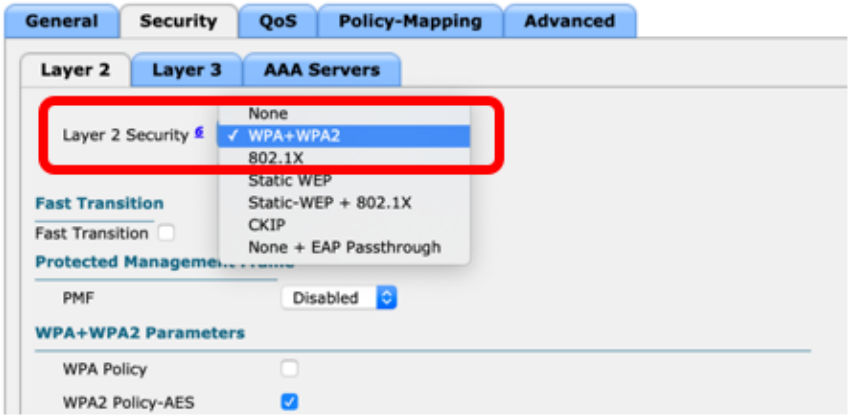
WPA2 PSK Configuration: WLAN Controllers

Step-3: Find the SSID for which you want to apply WPA2 security and select it for editing.

WPA2 PSK Configuration: WLAN Controllers

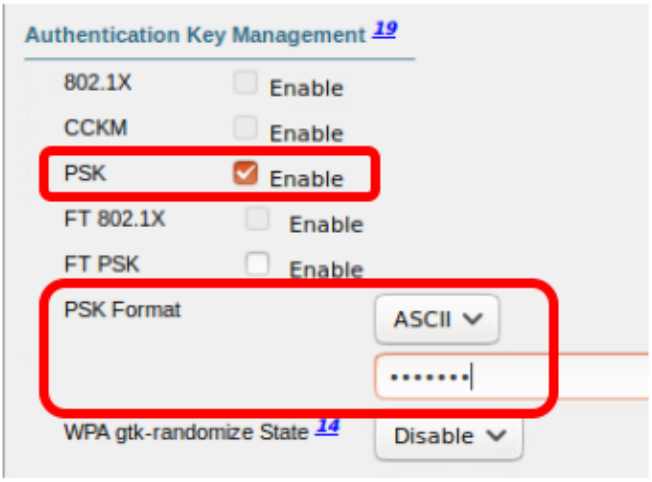
Step-4: Locate the “Security” or “Encryption” section for the selected SSID

WPA2 PSK Configuration: WLAN Controllers



Step-5: Select WPA2 as the encryption method (ensure AES is selected if not by default)

WPA2 PSK Configuration: WLAN Controllers



Step-6: Select PSK (or Pre-Shared Key) and type in your passphrase and save your changes..

Thanks for Watching!