Wi-Fi WPA

Why it's better then WEP

What is WPA?

Wi-Fi Protected Access (WPA) is a Wi-Fi security technology developed in response to the weaknesses of Wired Equivalent Privacy standards.

WPA2, in turn, is an upgraded form of WPA; since 2006, every Wi-Fi-certified product must use it.

The authentication and encryption features are a significant improvement over WEP.

Main features of WPA-2

Cryptographic algorithm	AES
Key size	128 bits
Encryption method	CCMP
Data integrity	CCMP
Keys for packets	Yes
IV length	48 bits

What is AES? Advanced Encryption Standard

Block encryption implementation

128-bit group encryption with 128, 192 and 256-bit key lengths

Symmetric algorithm requiring only one encryption and decryption key

Data security for 20-30 years

Worldwide access

No royalties

Easy overall implementation

What is TKIP?
Temporal Key Integrity Protocol

01

Boosting encryption strength

02

Preventing collision attacks without hardware replacement

03

Serving as a WEP code wrapper and also adding per-packet mixing of media access control (MAC) base keys and serial numbers

04

Assigning a unique 48-bit sequencing number to each packet

05

Utilizing the RC4 stream cipher - 128-bit encryption keys and 64-bit authentication keys

	Encryption	Authentication
WPA-Personal	TKIP	PSK
WPA2-Personal	DES-CCMP	PSK
WPA-Enterprise	TKIP	802.1X/EAP
WPA2-Enterprise	DES-CCMP	802.1X/EAP