Overcome WEP's Critical Flaws:

- WEP, introduced in 1997, was deeply insecure due to its use of the weak RC4 cipher, small 24-bit Initialization Vector (IV), static keys, and flawed authentication. These made WEP vulnerable to attacks like IV reuse, FMS, and Chopchop, allowing attackers to crack keys in minutes.
- WPA2 replaced WEP's RC4 with AES (Advanced Encryption Standard) and introduced CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), providing robust encryption and integrity protection, effectively eliminating WEP's vulnerabilities.

Improve on WPA's Temporary Solution:

- WPA, introduced in 2003, was a stopgap to address WEP's insecurities while maintaining compatibility with older hardware. It used TKIP (Temporal Key Integrity Protocol) with RC4, which was stronger than WEP but still had weaknesses, such as susceptibility to the Beck-Tews attack and limitations in cryptographic strength.
- WPA2 made AES-CCMP mandatory, offering a more secure and future-proof encryption standard. TKIP was retained as an optional fallback for compatibility but was phased out over time.

Meet Industry and Regulatory Demands:

- By the early 2000s, Wi-Fi adoption was growing rapidly, and secure wireless communication was critical for businesses, governments, and consumers. WEP's vulnerabilities and WPA's interim nature couldn't meet the security needs of sensitive applications.
- WPA2 was developed by the Wi-Fi Alliance, based on the IEEE 802.11i standard, to provide a standardized, high-security protocol that could be certified for compliance, ensuring trust across devices and networks.

Enhance Encryption and Authentication:

- WPA2 introduced AES, a military-grade encryption standard, which is far more resistant to cryptographic attacks than RC4. CCMP added per-packet key mixing and strong message integrity checks, preventing data tampering.
- It supported robust authentication methods, including 802.1X/EAP for enterprise networks (using a RADIUS server) and PSK (Pre-Shared Key) for personal networks, improving access control over WEP's weak Shared Key authentication.

Ensure Long-Term Security and Scalability:

- WPA2 was designed to be a long-term solution, capable of securing Wi-Fi networks as data rates and network complexity increased. Its use of AES-CCMP provided a foundation for secure communication that remained effective for over a decade.