GLOBAL EDGE
Intelligence Of Things™

Wireless LAN Security

Anvesh Jain P

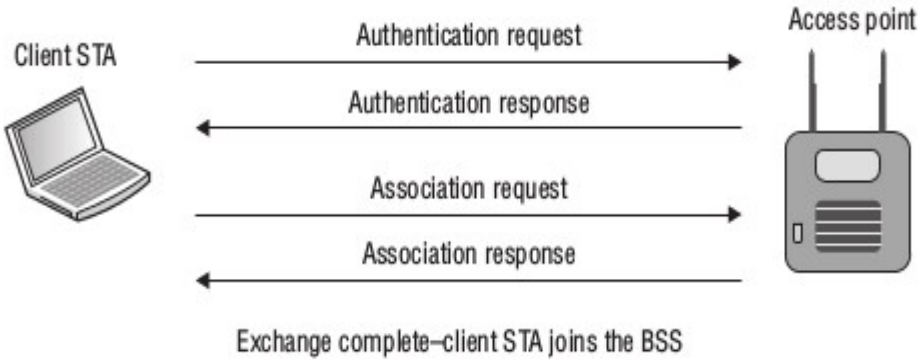
Contents

- Authentication
- WLAN encription methods
- WPA/WPA2 .
- Robust Security Networks.
- Four – way Handshake.

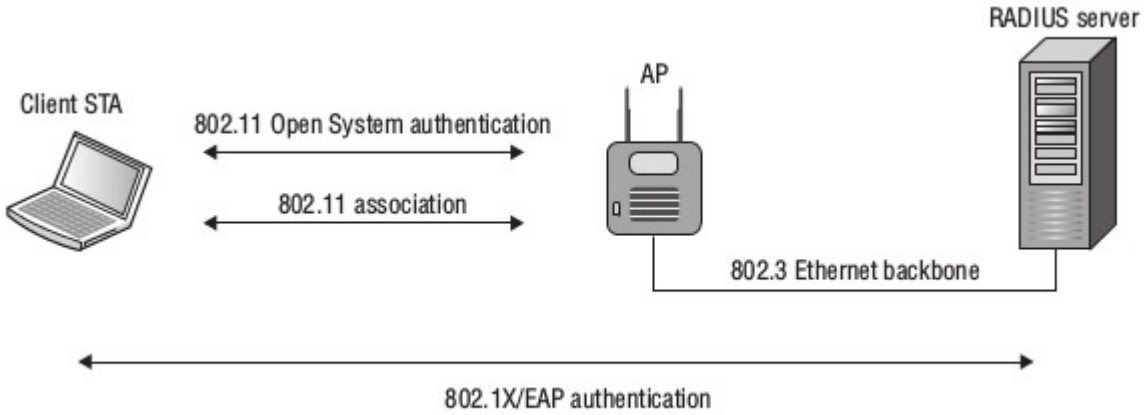
Authentication

- Authentication is the first of two steps required to connect to the 802.11 basic service set.
- The 802.11 authentication merely establishes an initial connection between the client and the access point
- The 802.11-2007 standard specifies two different methods of authentication:
  a)Open system Authentication.
  b)Shared key authentication,

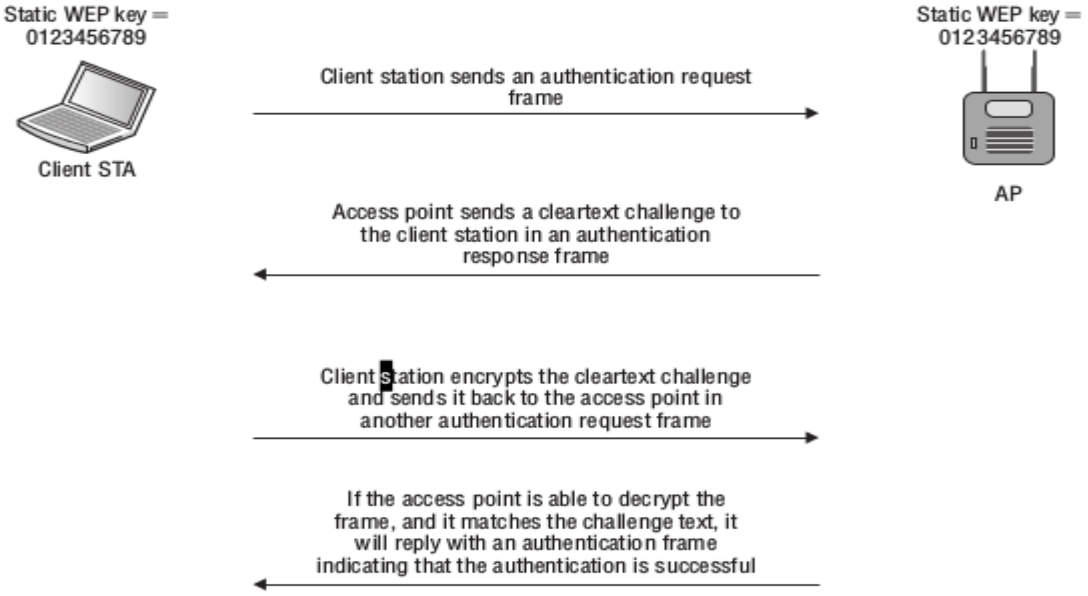
Open system Authentication



Open system and 802.11X/EAP Authentication



Shared Key Authentication



WLAN encryption methods

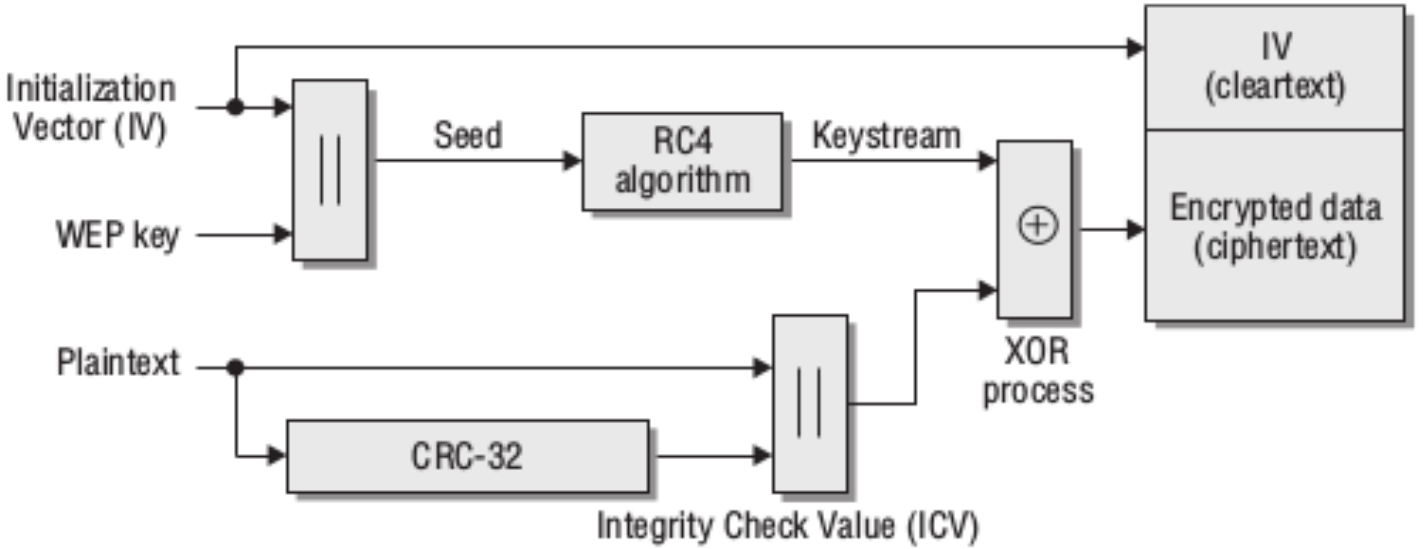
- The 802.11-2007 standard defines three encryption methods that operate at layer 2 of the OSI model:
  - Wired Equivalent privacy(WEP).
  - Temporary Key Integration Protocol(TKIP).
  - CTR with CBC-MAC Protocol(CCMP).

- WEP, TKIP, CCMP are used to encrypt the MSDU payload of an 802.11 data frame.

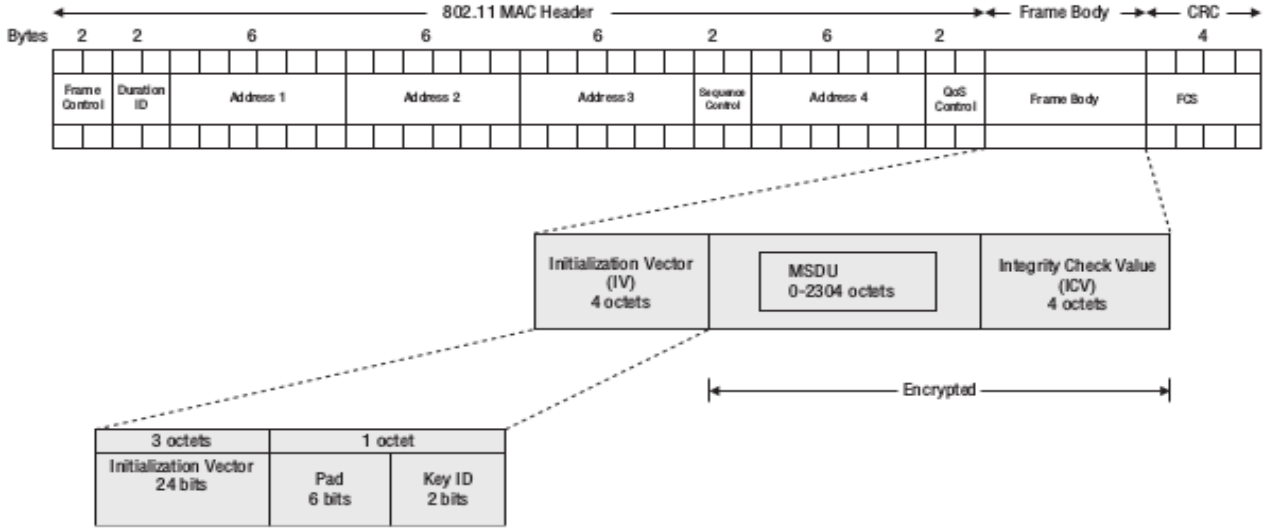
Wired Equivalent Privacy

- Wired Equivalent Privacy is a layer 2 security protocol that uses the RC4 streaming cipher.
- 64-bit WEP uses a secret 40-bit static key, which is combined with a 24-bit number selected by the card’s device drivers.
- This 24-bit number, known as the initialization vector(IV)
- Pseudo random RC4 algorithm is used to generate keystream.
- Keystream then combined with the plain-text data bits by using a Boolean XOR process.

- WEP encryption process



- WEP MPDU Format



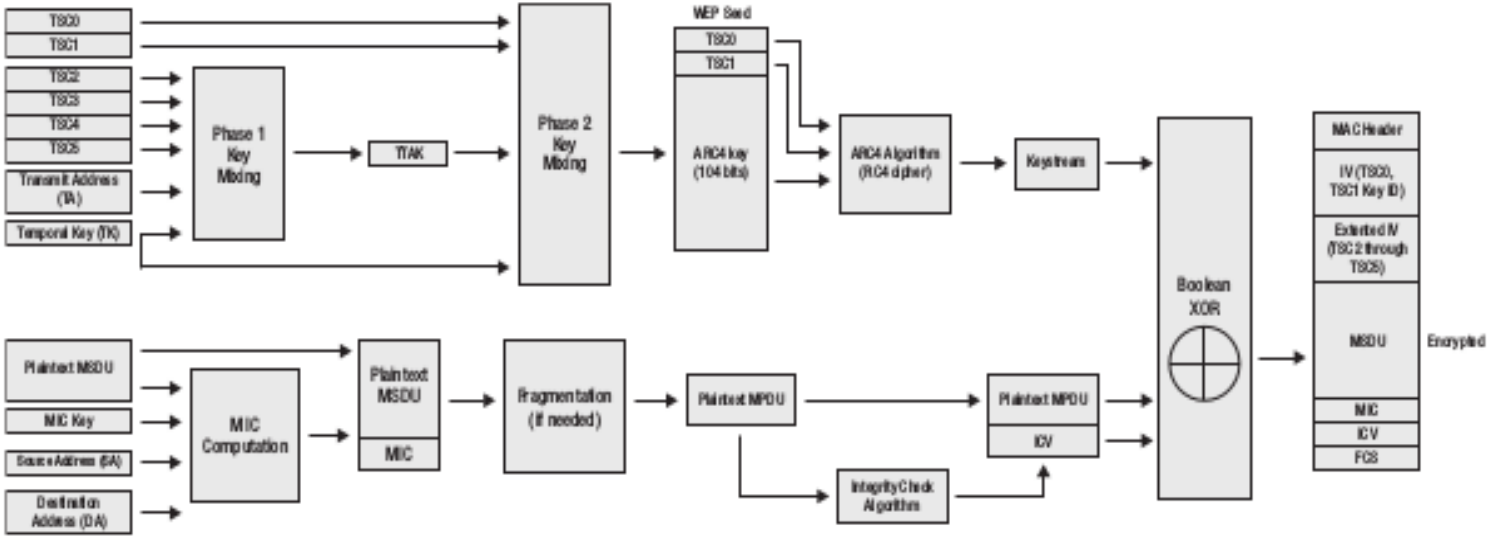
Temporary Key Integration Protocol

- TKIP is an enhancement of WEP.
- TKIP uses the ARC4 algorithm for performing its encryption and decryption processes.
- TKIP uses dynamically created encryption keys as opposed to the static keys.
- Any two radios use a 4-Way Handshake process to create dynamic unicast keys that are unique to those two radios

Temporary Key Integration Protocol

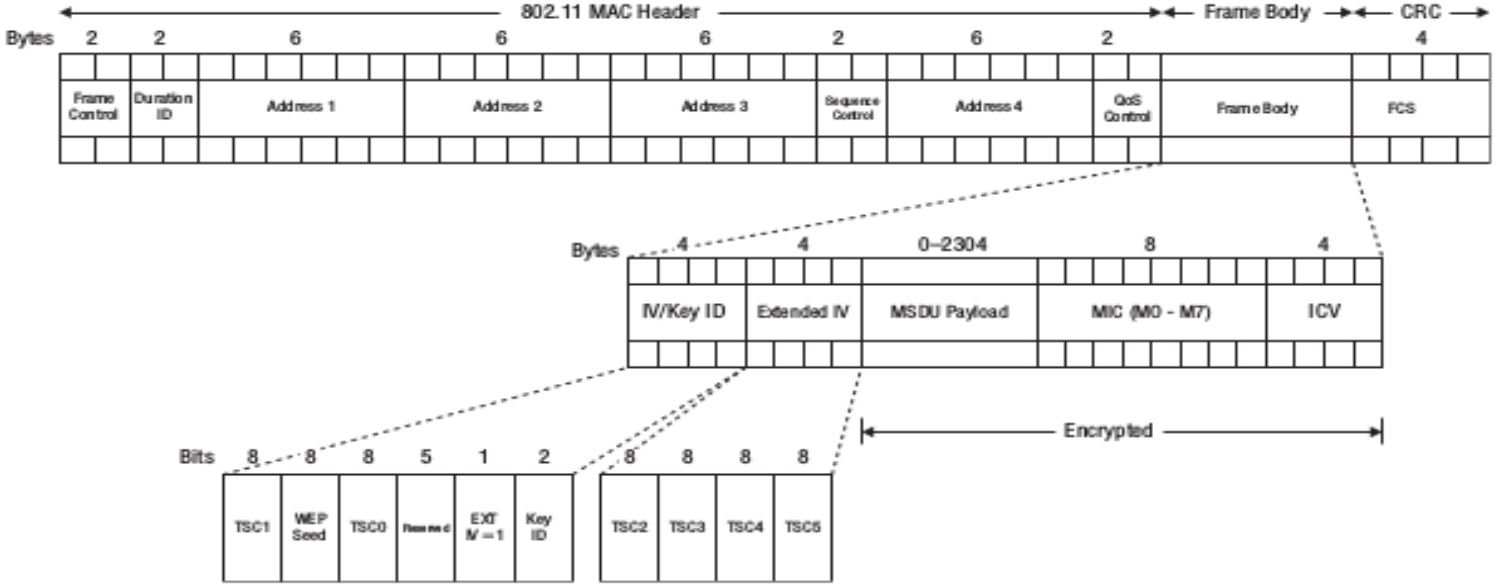
- TKIP starts with a 128-bit temporal key.
- The 128-bit temporal key is a dynamically generated key that comes from a 4-Way Handshake creation process.
- This key is identical on the AP and client pair.
- he 128-bit temporal key can either be a pairwise transient key (PTK) used to encrypt unicast traffic
- or a group temporal key (GTK) used to encrypt broadcast and multicast traffic.

TKIP encryption and data integrity process



Temporary Key Integration Protocol

- TKIP MPDU

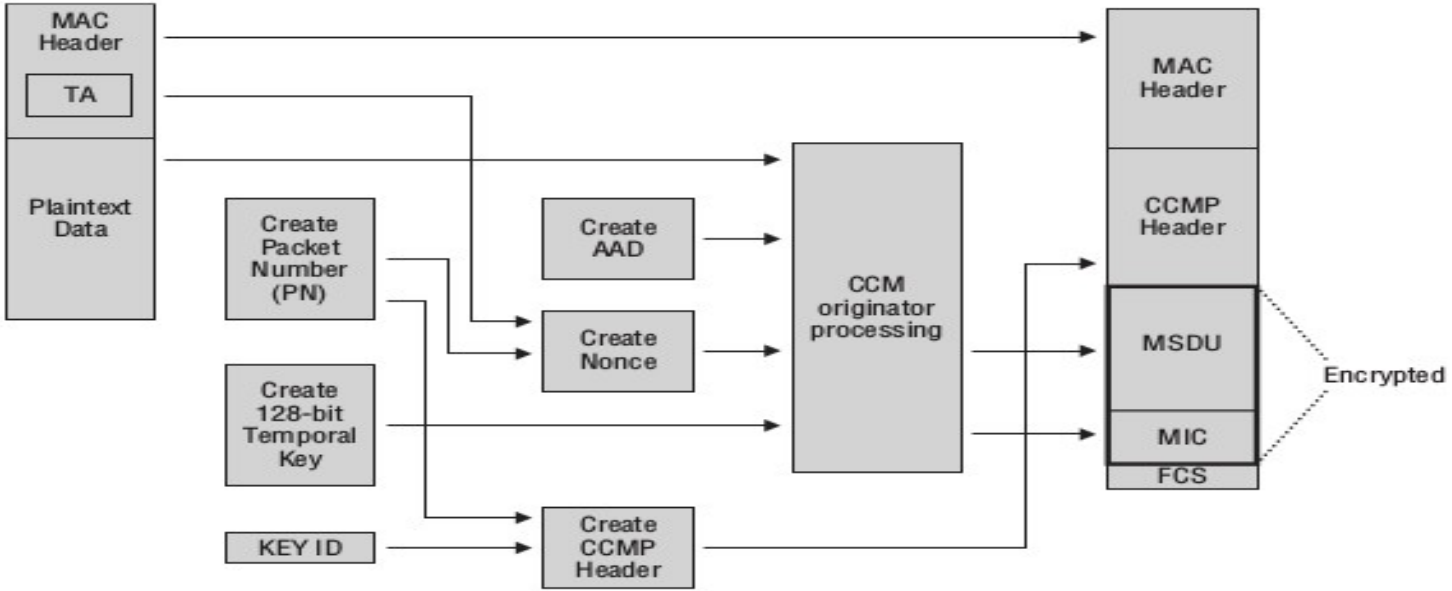


CTR with CBC-MAC Protocol(CCMP)

- The full phrase of counter mode with the Cipher-Block Chaining Message Authentication Code protocol is represented by the acronym of CCMP.
- certain fields in the MPDU header are used to construct the additional authentication data (AAD).
- This information is used for data integrity of portions of the MAC header.
- CTR is used to provide data confidentiality.
- The CBC-MAC is used for authentication and integrity.

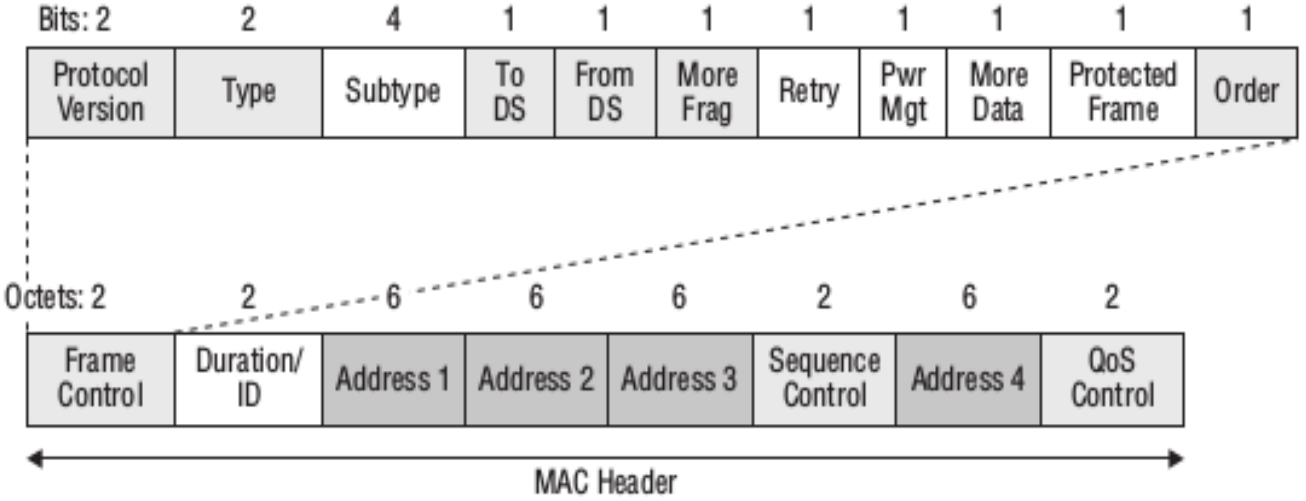
CTR with CBC-MAC Protocol(CCMP)

- CCMP encryption and data integrity process



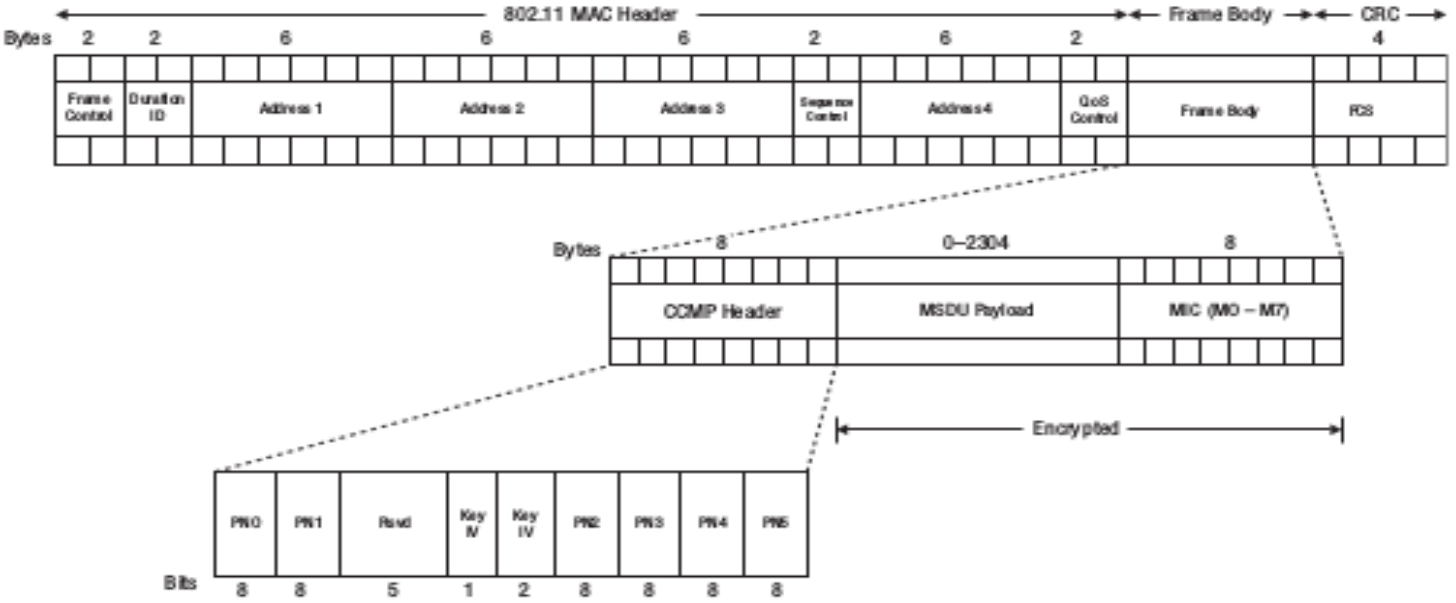
CTR with CBC-MAC Protocol(CCMP)

- Additional authentication data



CTR with CBC-MAC Protocol(CCMP)

- CCMP MPDU



Wifi Protected Access(WPA)

- Temporal Key Integrity Protocol (TKIP) was adopted for WPA.
- WPA also includes a Message Integrity Check.
- WPA2 is the upgraded version of WPA which uses CCMP/AES encryption.
- The various protection mechanisms of WPA are.

  1) WPA-Personal(WPA-PSK(Pre shared key))
  2) WPA-Enterprise(WPA-802.11X mode).
  3) Wifi Protected setup

Robust security networks

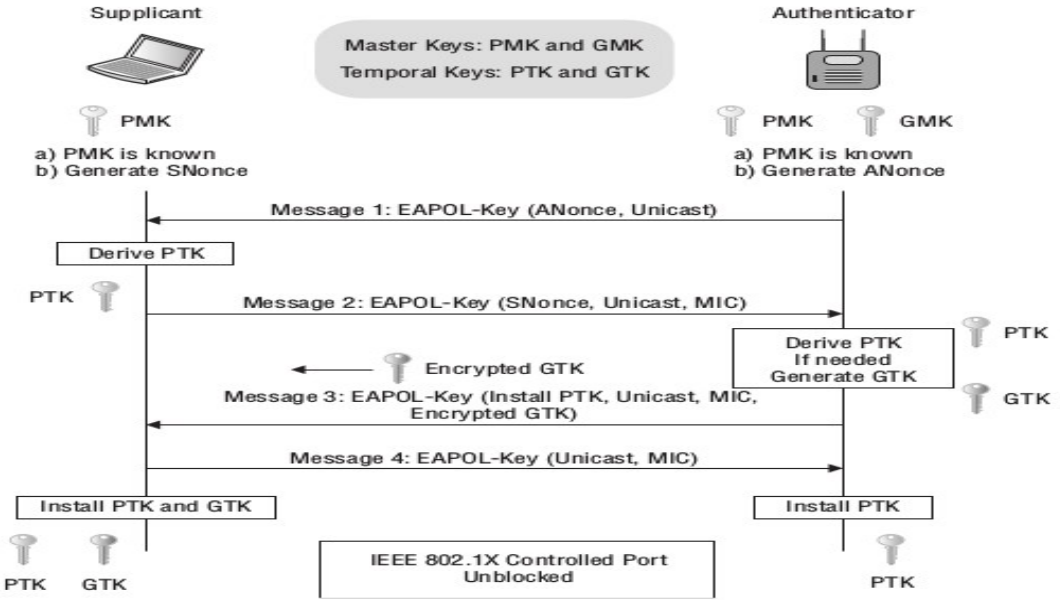
- The 802.11-2007 standard defines what is known as a robust security network (RSN) and robust security network associations (RSNAs).
- A robust security network association (RSNA) requires two 802.11 stations (STAs) to establish procedures to
  - Authenticate
  - Associate
  - create dynamic encryption keys through a process known as the 4-Way Handshake
- CCMP/AES encryption is the mandated encryption method, while TKIP/RC4 is an optional encryption method.

4-WAY HANDSHAKE

- The 4-Way Handshake is a final process used to generate pairwise transient keys for encryption of unicast transmissions
- and a group temporal key for encryption of broadcast/multicast transmissions.
- The 4-Way Handshake uses four EAPOL-Key frame messages between the authenticator and the supplicant
- 802.1X/EAP authentication is completed when the access point sends an EAP-Success frame and the AP can now initiate the 4-Way Handshake

Four way Handshake

- The 4 way handshake



Large enough to Deliver, Small enough to Care

Global Village
IT SEZ
Bangalore

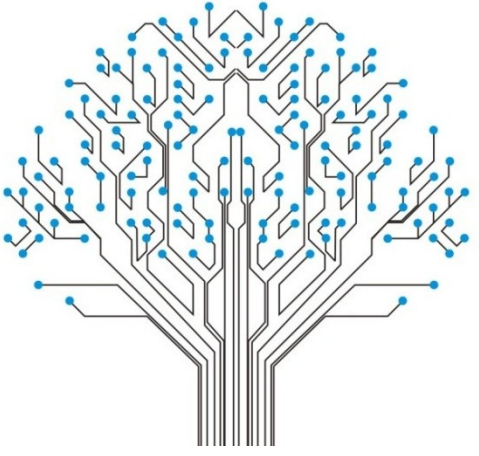
South Main Street
Milpitas
California

Raheja Mindspace
IT Park
Hyderabad

www.globaledgesoft.com

GLOBAL EDGE
Intelligence Of Things™

Thank you



Fairness

Learning

Responsibility

Innovation

Respect