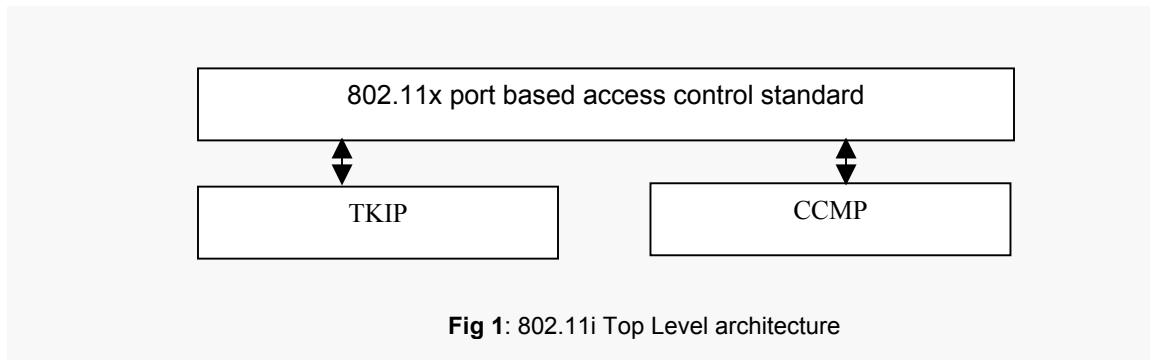


## Secure Wireless with 802.11i

802.11i is a draft internet standard from the IEEE 802.11i committee that aims to solve the security flaws that haunt the 802.11a and 802.11b wireless networking standards. With wireless networks (such as 802.11b) becoming increasingly popular in residential and commercial environments, and with the WEP (Wireless Equivalence Privacy standard, the security standard of the current wireless networks) being exposed several times to flaws, the current wireless networks are vulnerable to hackers located within range. 802.11i addresses this problem by providing for better security with difficult to break encryption techniques and algorithms.

### 802.11i architecture

The 802.11i specification can be viewed as three modules in two layers. Encryption algorithms form the lower layer with TKIP and CCMP. Above the encryption algorithms is the 802.11x, which is a port based access control standard. The three modules work together to form the security system.



The key features of 802.11i are:

- Supports two encryption standards
  - Encryption based on AES (Advanced Encryption Standard) with 128-bit strong key cipher
  - TKIP encryption
- CBC-MAC cipher algorithm (CCMP) handles header and data integrity
- Change in cipher keys over time
- EAP (Extensible Authentication Protocol) for key management

Advanced Encryption Standard is a symmetric iterated block cipher (uses the same key for both encryption and decryption). The algorithm makes multiple passes over the input data and outputs fixed length blocks. The AES algorithm in 802.11i uses a 128-bit encryption key. This AES based encryption standard is mandatory for 802.11i devices.

TKIP is an encryption standard designed to address all known vulnerabilities in the existing wireless standards while maintaining backward compatibility. The key features of TKIP include:

- 48-bit IV and IV sequence counter to protect against address replay attacks
- Weak key attack protection by using techniques like per packet key mixing
- Countermeasures to prevent hackers from knowing sufficient information to break a cipher key
- Cryptographic checksum protects against forgery attacks

TKIP is optional in 802.11i devices but provides increased security and privacy when used.

EAP-TLS (RFC-2284, RFC-2246, RFC-2716) is the de facto authentication method in 802.11i. EAP uses public certificates as preventive measure against spoofing with access points. In this technique, the network verifies the user and the user also verifies the network, thus ensuring maximum security.

### **802.11i Standard Operational Phases (SOP)**

The Standard Operational Phases of a 802.11i based network client are as follows:

- The client and access-point exchange messages for capability identification
- Access-point advertises its authentication capabilities to the client
- Authentication is performed producing a master key (MK) that exists between the client and the authentication server.
- A pair wise master key (PMK) is created from the master key for use by the client and the access-point. Also the Temporal key (TK) is created that is actually used to secure data communications between client and the access-point

### **In Conclusion**

802.11i specification aims to make wireless networks more secure. The algorithms in the standard, though very secure in nature, make it costly and complicated. Any 802.11i enabled device requires a separate cryptographic processor to perform the encryption algorithms in real-time. But the feature benefits far outweigh the cost disadvantage.