# TABLE 7.1
# IEEE 802.11 TERMINOLOGY

| | |
|---|---|
| Access point (AP) | Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations. |
| Basic service set (BSS) | A set of stations controlled by a single coordination function. |
| Coordination function | The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs. |
| Distribution system (DS) | A system used to interconnect a set of BSSs and integrated LANs to create an ESS. |
| Extended service set (ESS) | A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs. |
| MAC protocol data unit (MPDU) | The unit of data exchanged between two peer MAC entities using the services of the physical layer. |
| MAC service data unit (MSDU) | Information that is delivered as a unit between MAC users. |
| Station | Any device that contains an IEEE 802.11 conformant MAC and physical layer. |


**Figure 7.4 General IEEE 802 MPDU Format**

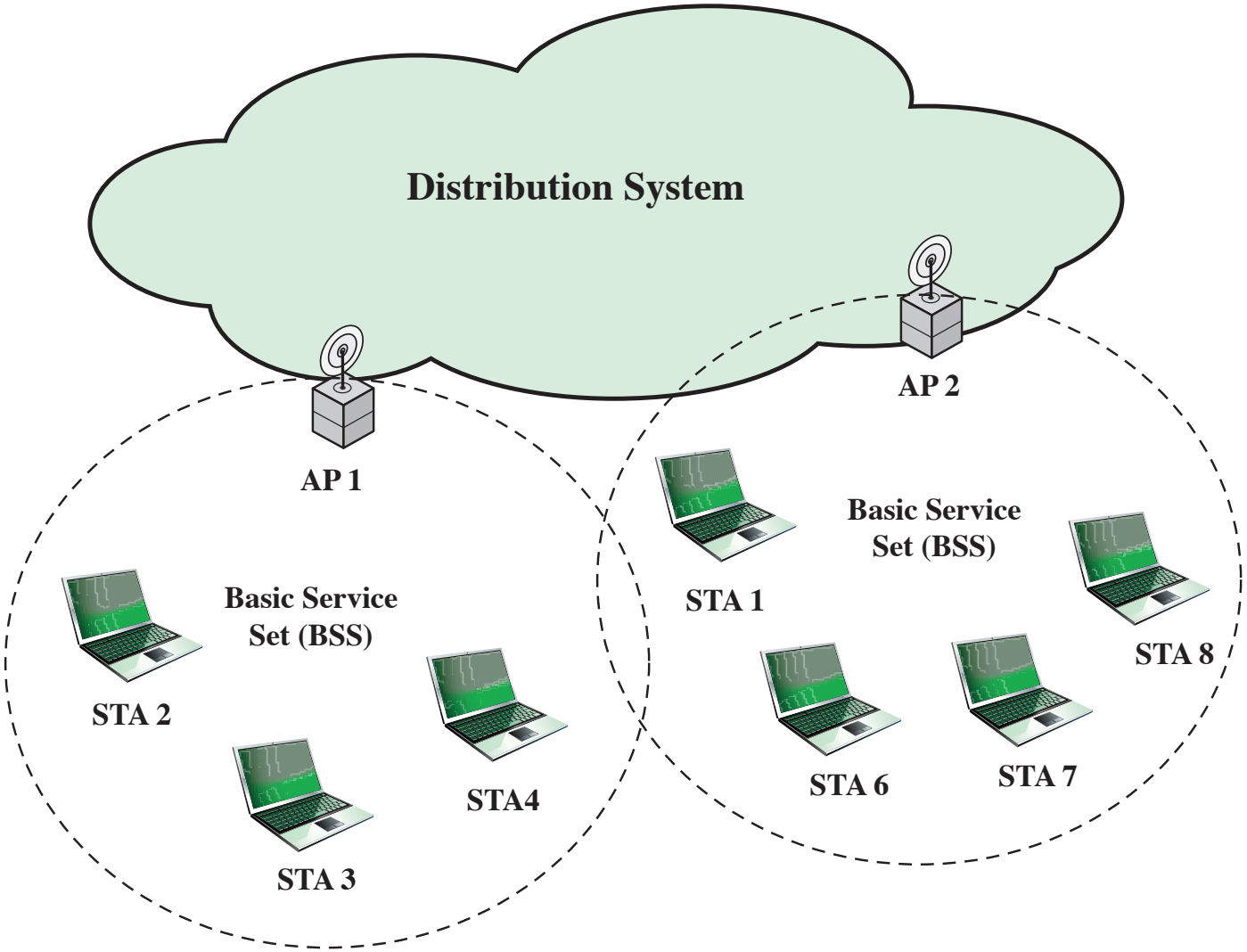
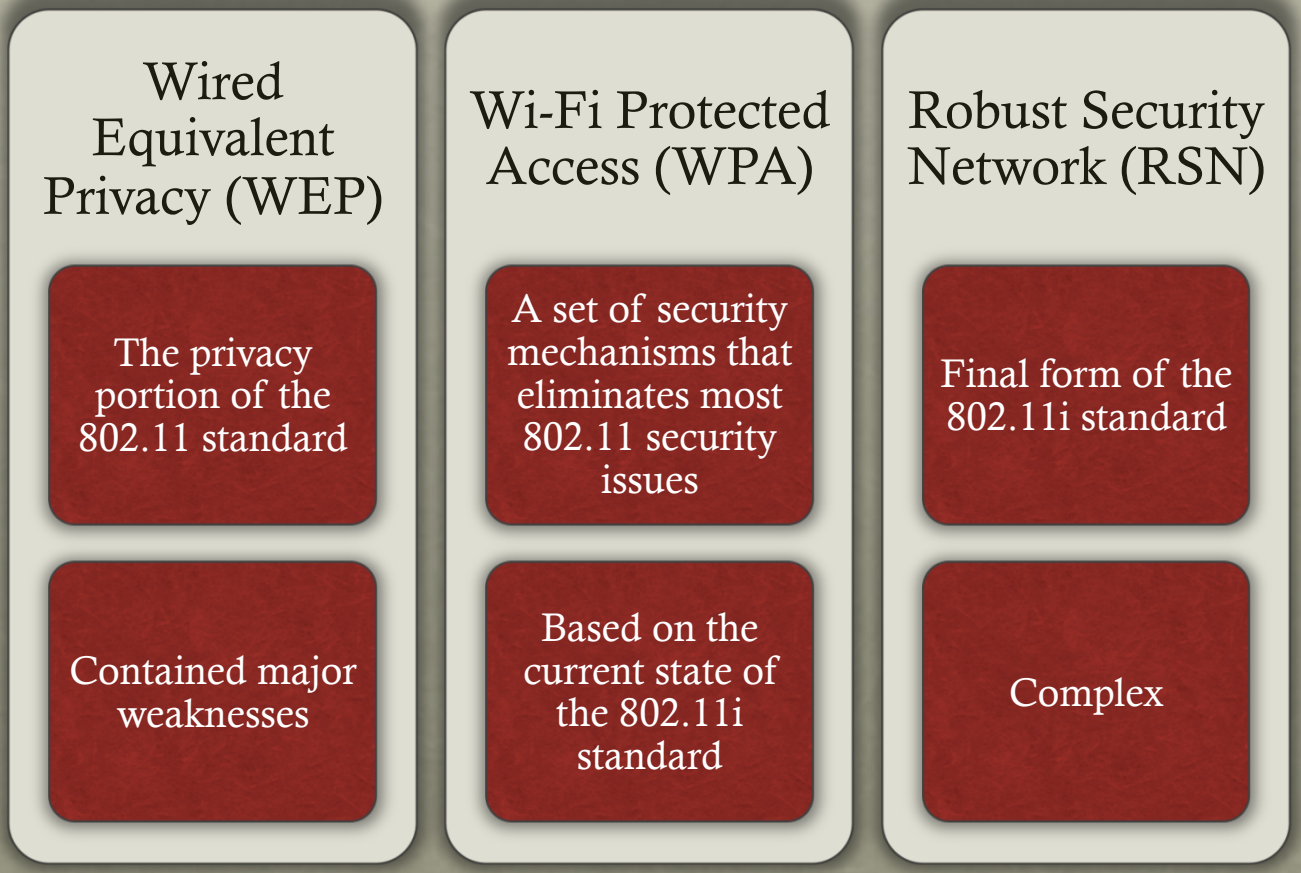
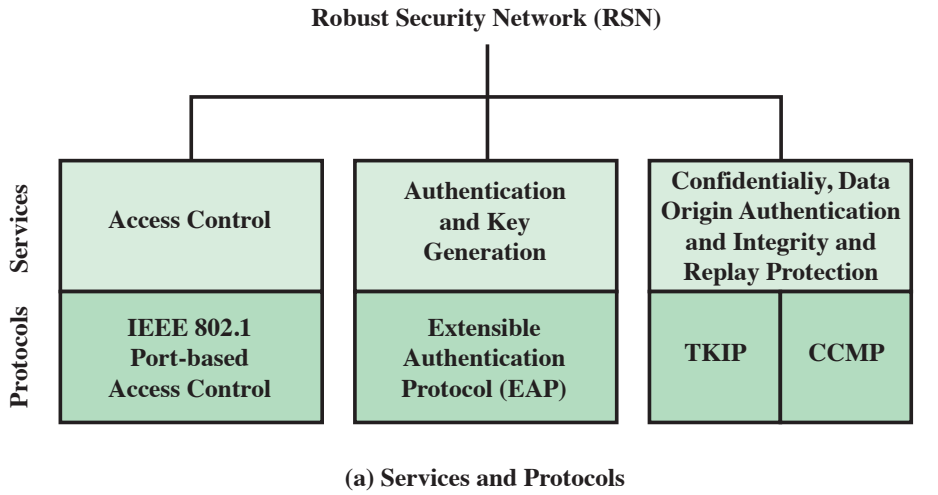



**Figure 7.5 IEEE 802.11 Extended Service Set**

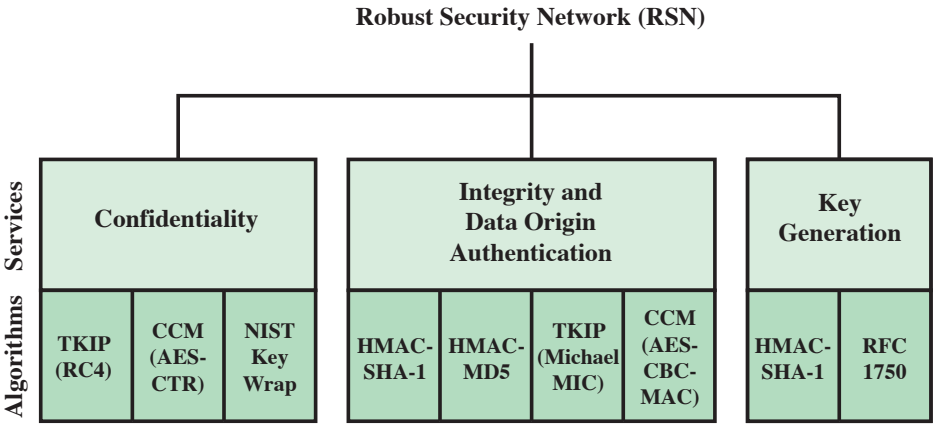
# IEEE 802.11i Wireless LAN Security

- There is an increased need for robust security services and mechanisms for wireless LANs





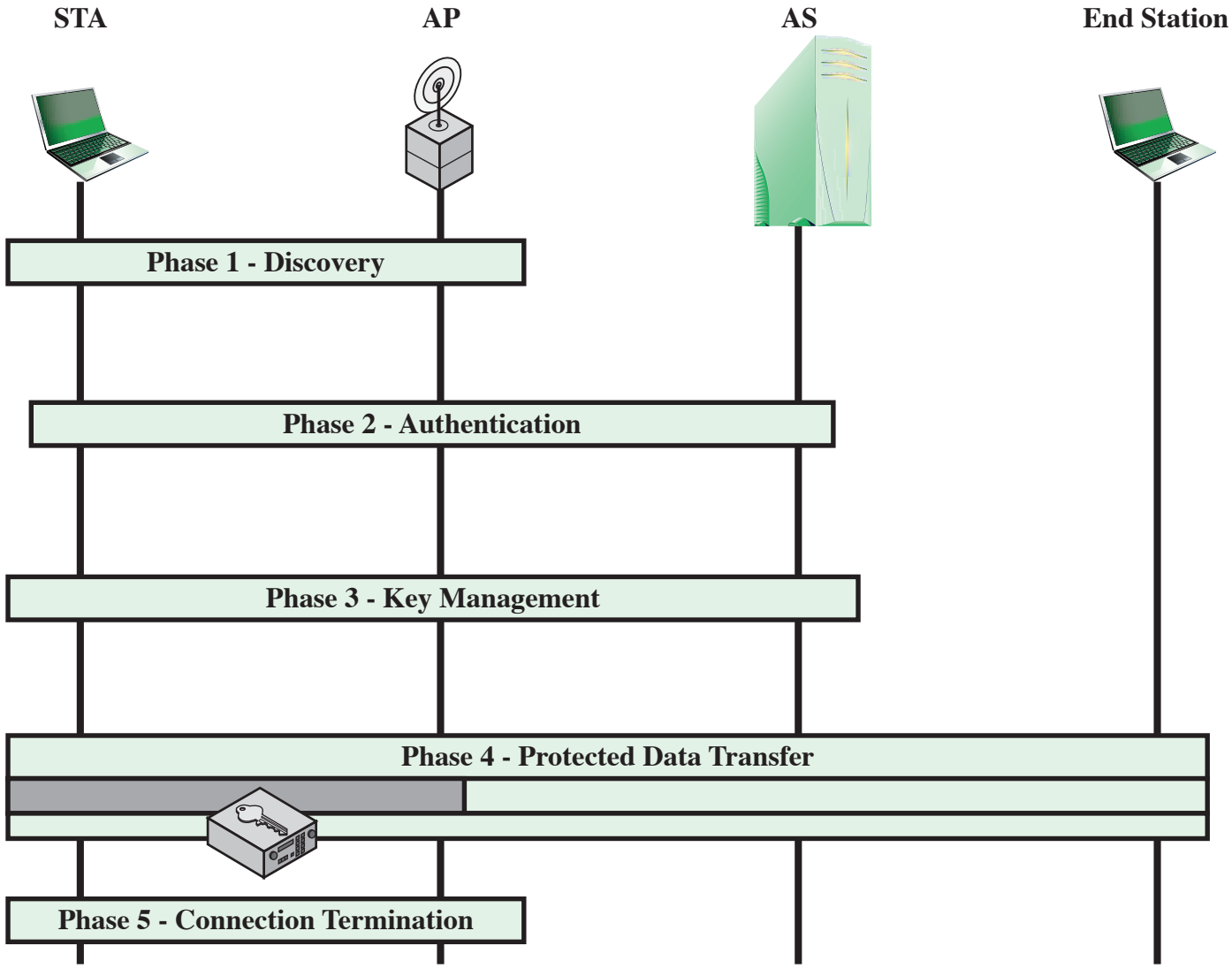

(a) Services and Protocols




(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

**Figure 7.6 Elements of IEEE 802.11i**




Only between STAs to AP. E-2-E security needed outside BSS across Distribution Systems
End Station to AP not secure in this example: For E-2-E Security End station run 802.11i.

**Figure 7.7 IEEE 802.11i Phases of Operation**

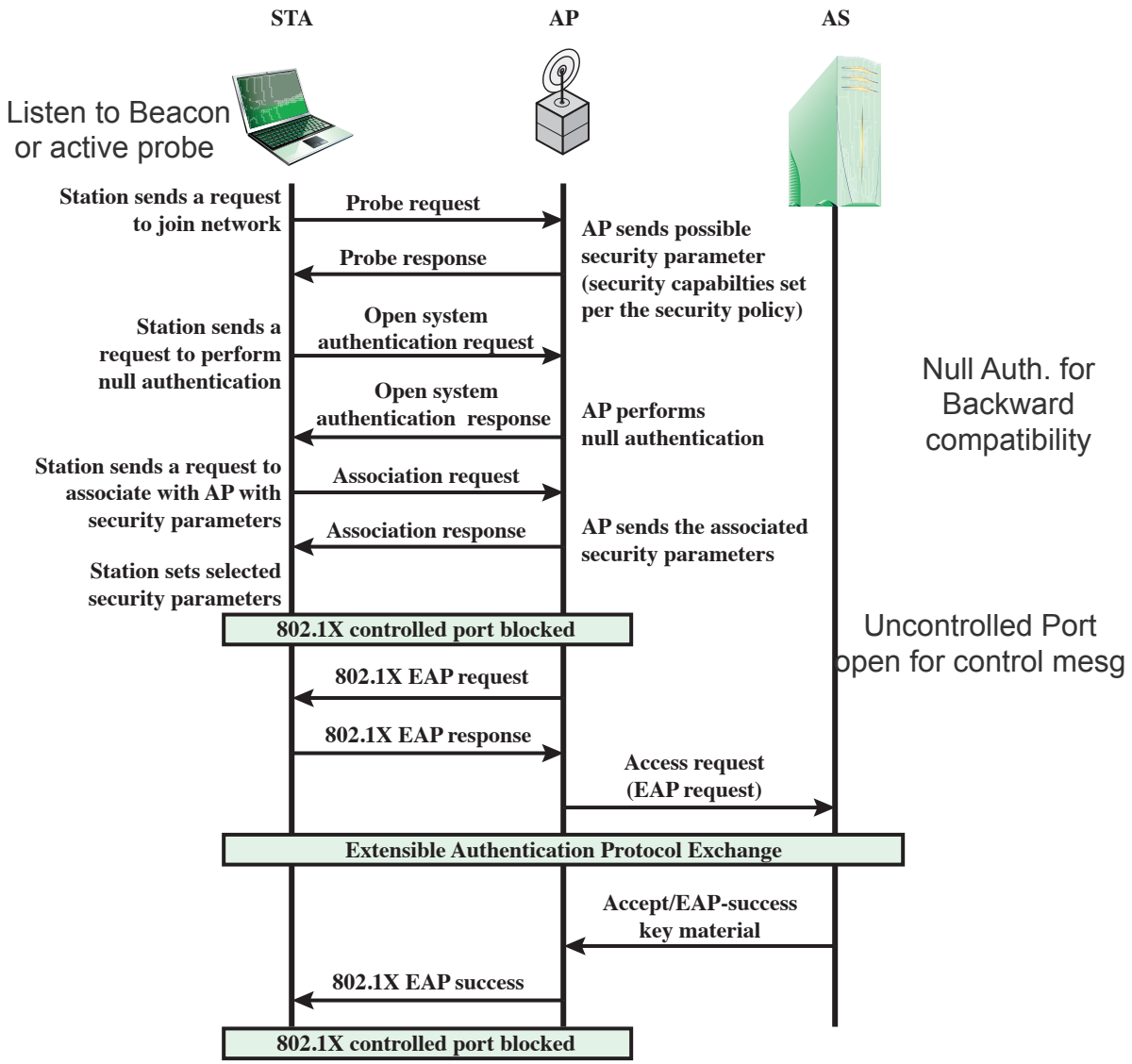
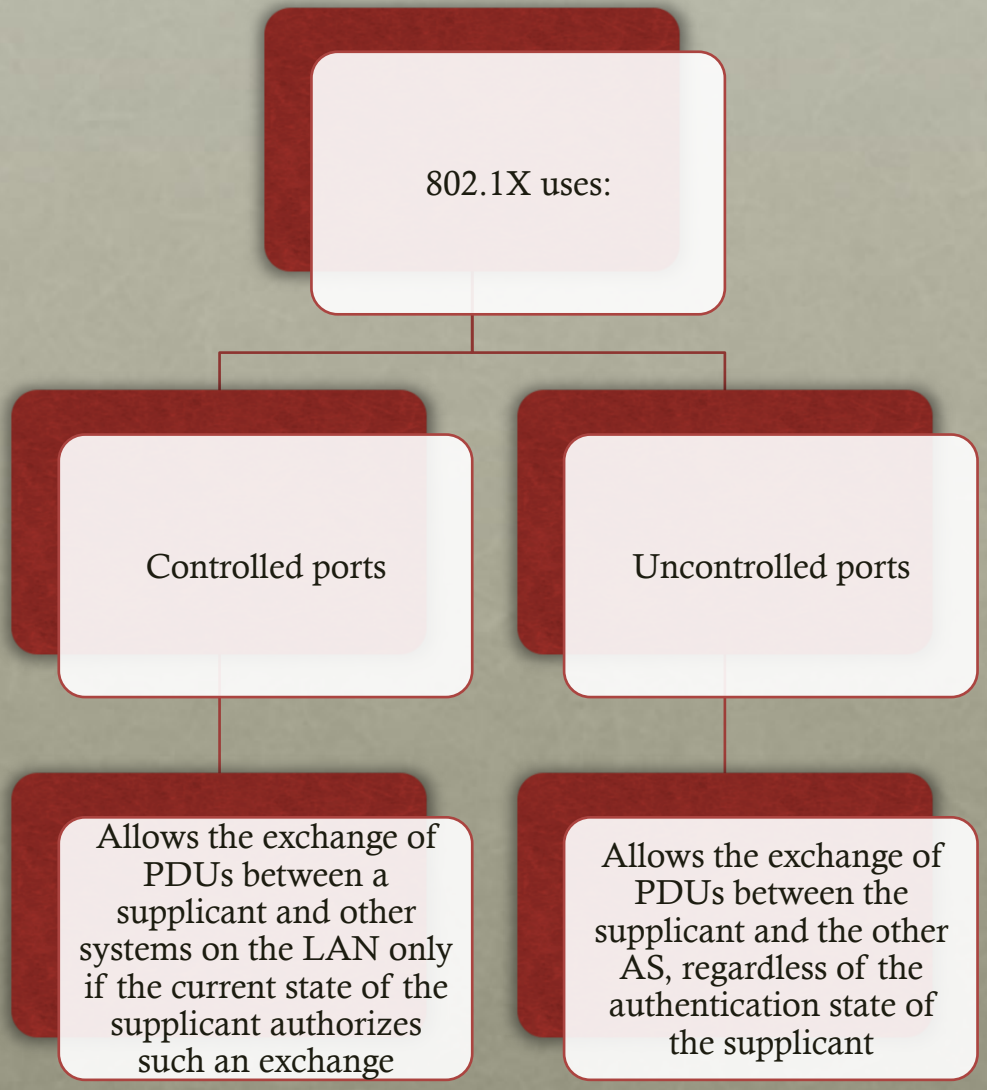



**Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association**

# IEEE 802.1X RECAP

- Port-Based Network Access Control
- The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard

STA = Supplicant
AP = Authenticator



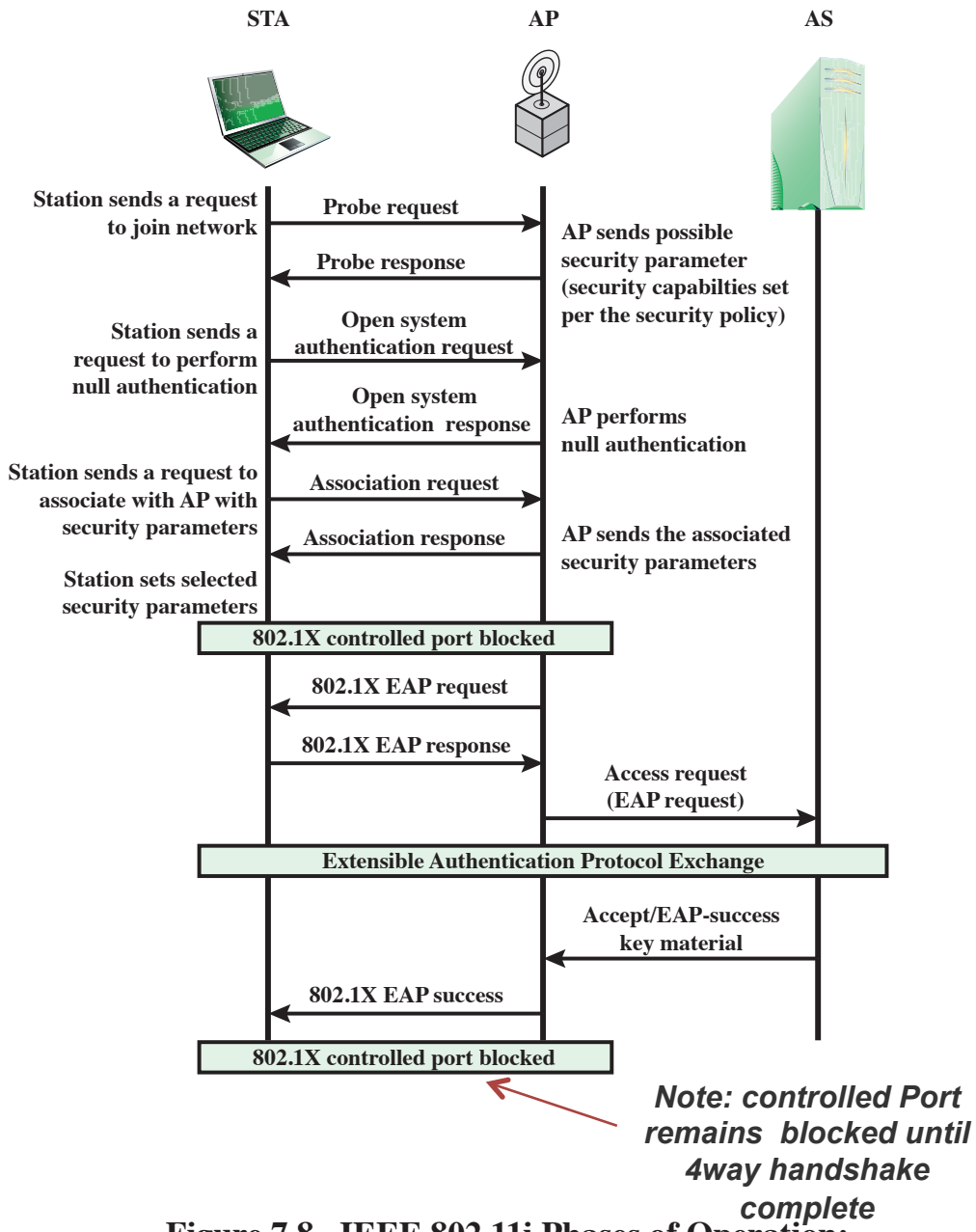
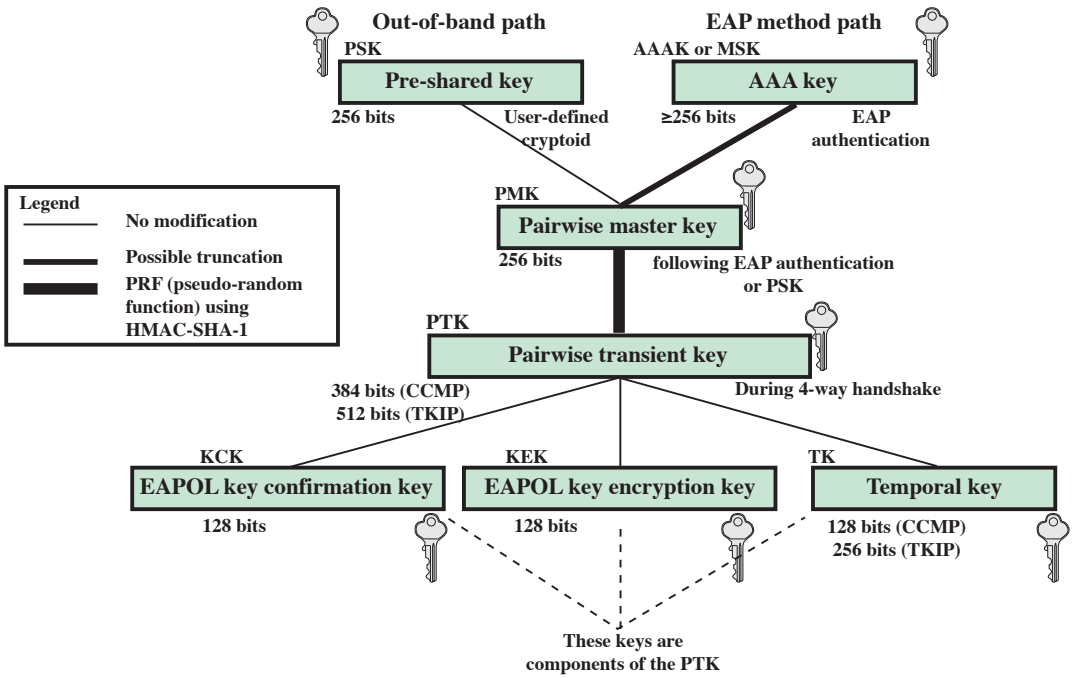
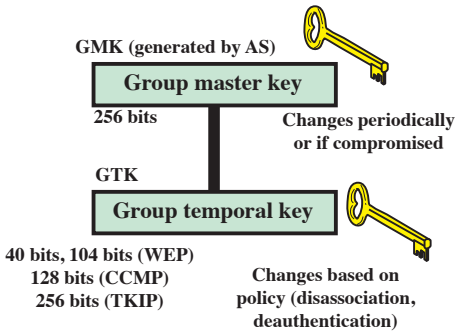



**Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association**




(a) Pairwise key hierarchy




(b) Group key hierarchy

**Figure 7.9 IEEE 802.11i Key Hierarchies**

# Table 7.3

## IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

| Abbrev-iation | Name | Description / Purpose | Size (bits) | Type |
|---|---|---|---|---|
| AAA Key | Authentication, Accounting, and Authorization Key | Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK. | ≥ 256 | Key generation key, root key |
| PSK | Pre-Shared Key | Becomes the PMK in pre-shared key environments. | 256 | Key generation key, root key |
| PMK | Pairwise Master Key | Used with other inputs to derive the PTK. | 256 | Key generation key |
| GMK | Group Master Key | Used with other inputs to derive the GTK. | 128 | Key generation key |
| PTK | Pair-wise Transient Key | Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key. | 512 (TKIP)<br>384 (CCMP) | Composite key |
| TK | Temporal Key | Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic. | 256 (TKIP)<br>128 (CCMP) | Traffic key |
| GTK | Group Temporal Key | Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic. | 256 (TKIP)<br>128 (CCMP)<br>40, 104 (WEP) | Traffic key |
| MIC Key | Message Integrity Code Key | Used by TKIP's Michael MIC to provide integrity protection of messages. | 64 | Message integrity key |
| EAPOL-KCK | EAPOL-Key Confirmation Key | Used to provide integrity protection for key material distributed during the 4-Way Handshake. | 128 | Message integrity key |
| EAPOL-KEK | EAPOL-Key Encryption Key | Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake. | 128 | Traffic key / key encryption key |
| WEP Key | Wired Equivalent Privacy Key | Used with WEP. | 40, 104 | Traffic key |

# PAIRWISE KEYS

- **Used for communication between a pair of devices, typically between a STA and an AP**
  - These keys form a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time
- **Pre-shared key (PSK)**
  - A secret key shared by the AP and a STA and installed in some fashion outside the scope of IEEE 802.11i
- **Master session key (MSK)**
  - Also known as the AAAK, and is generated using the IEEE 802.1X protocol during the authentication phase
- **Pairwise master key (PMK)**
  - Derived from the master key
  - If a PSK is used, then the PSK is used as the PMK; if a MSK is used, then the PMK is derived from the MSK by truncation
- **Pairwise transient key (PTK)**
  - Consists of three keys to be used for communication between a STA and AP after they have been mutually authenticated
  - Using the STA and AP addresses in the generation of the PTK provides protection against session hijacking and impersonation; using nonces provides additional random keying material

# PTK PARTS

- The three parts of the PTK are:

**EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK)**

- Supports the integrity and data origin authenticity of STA-to-AP control frames during operational setup of an RSN
- It also performs an access control function: proof-of-possession of the PMK

**EAPOL Key Encryption Key (EAPOL-KEK)**

- Protects the confidentiality of keys and other data during some RSN association procedures

**Temporal Key (TK)**

- Provides the actual protection for user traffic

# GROUP KEYS

- Group keys are used for multicast communication in which one STA sends MPDUs to multiple STAs
  - Group master key (GMK)
    - Key-generating key used with other inputs to derive the GTK
  - Group temporal key (GTK)
    - Generated by the AP and transmitted to its associated STAs
    - Distributed securely using the pairwise keys that are already established
    - Is changed every time a device leaves the network

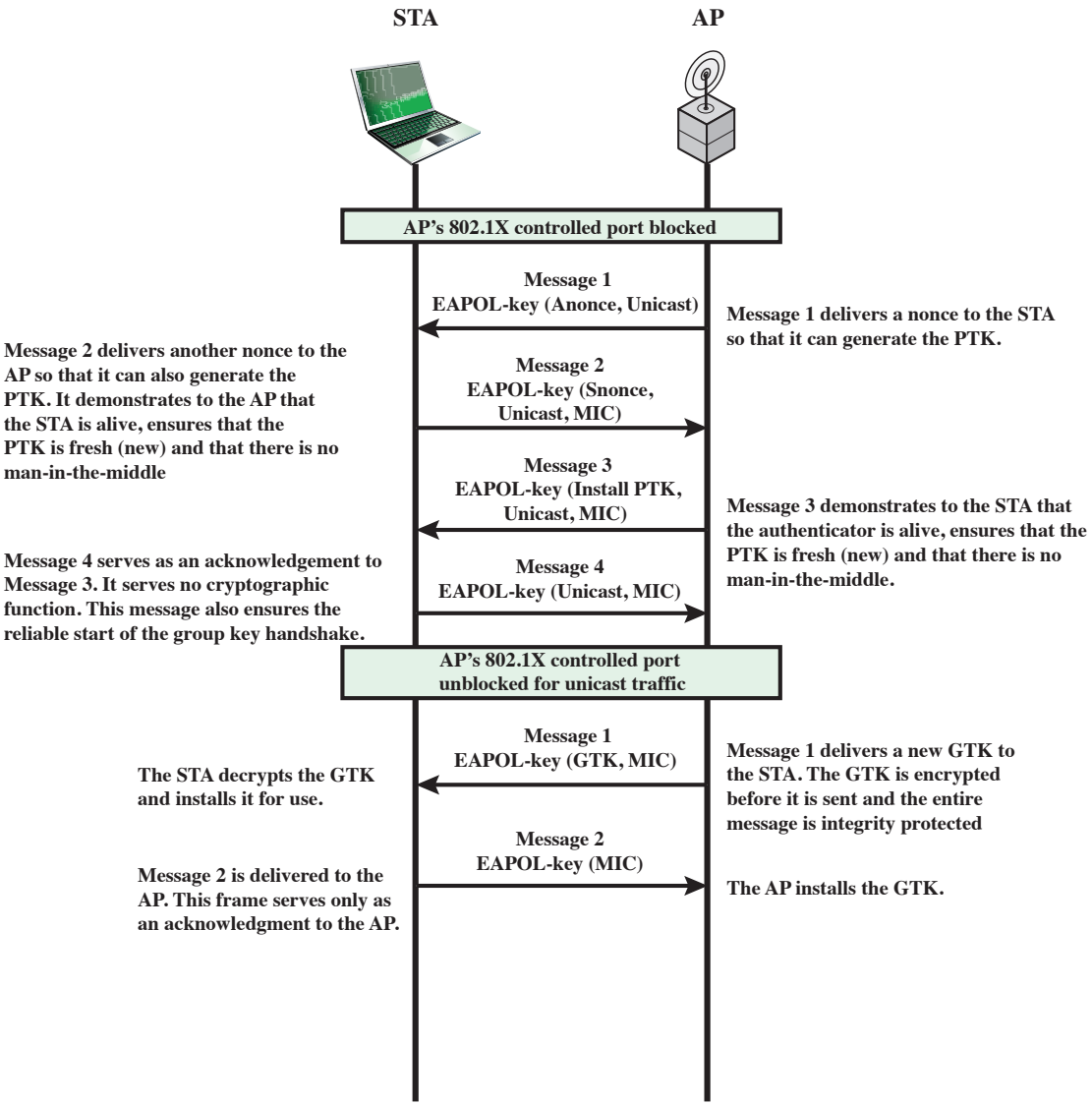
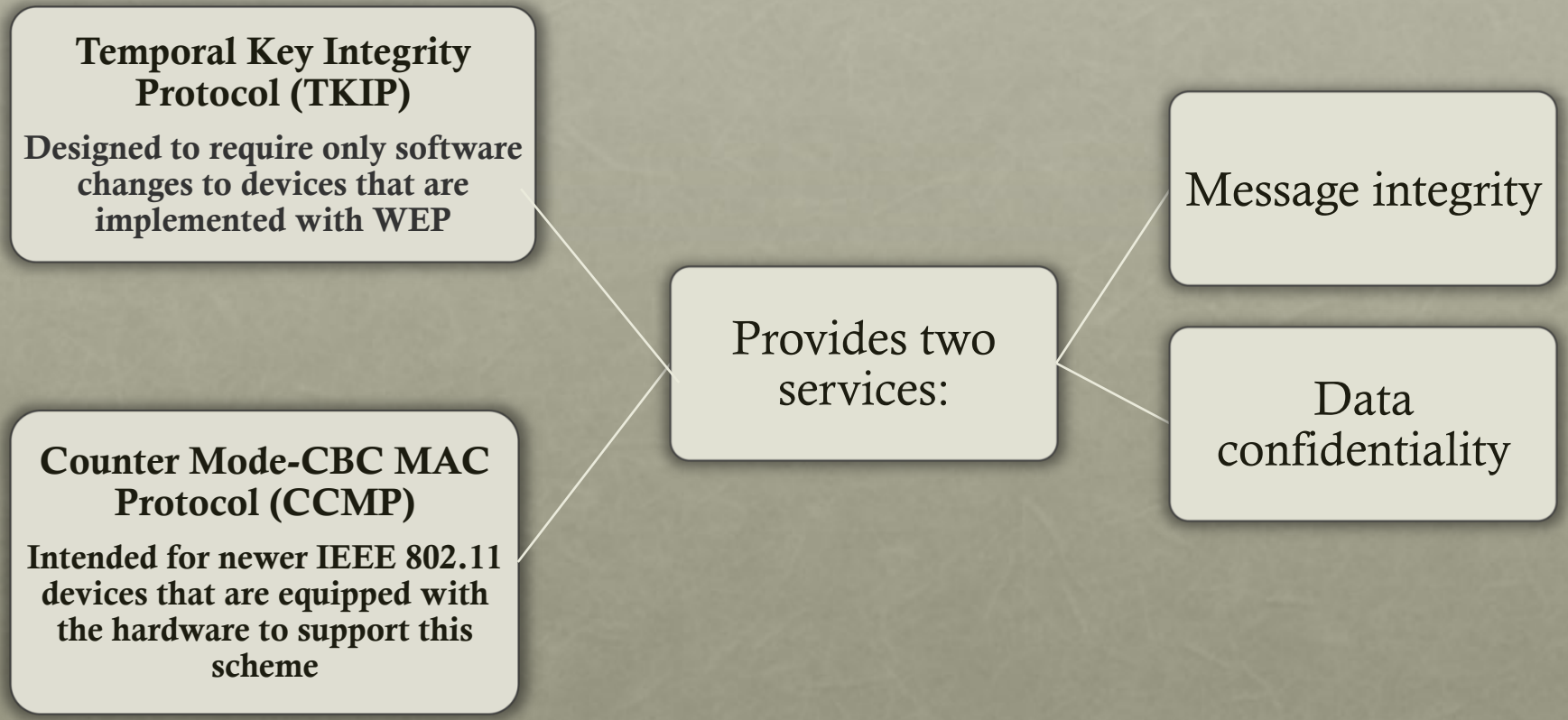



**Figure 7.10 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake**

# PROTECTED DATA TRANSFER PHASE

- IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs:



# REFERENCES

- **These foils are from Network Security Essentials, Applications and Standards – 5th Ed**, Chapter 7 Section 7.3 and 7.4