BSCIT

Network Security

Unit 5

Wireless Network Security

Unit 5

Wireless Network Security

5 Topics

1. IEEE 802.11 Wireless LAN Overview
2. IEEE 802.11i Wireless LAN Security
3. Wireless Application Protocol Overview
4. Wireless Transport Layer Security
5. WAP End-to-End Security

1. IEEE 802.11 Wireless LAN Overview

IEEE 802.11 Wireless LAN Overview (4)

1. The Wi-Fi Alliance
2. IEEE 802 Protocol Architecture
3. IEEE 802.11 Network Components and Architectural Model
4. IEEE 802.11 Service

1. The Wi-Fi Alliance

- IEEE - Institute of Electrical and Electronics Engineers
- IEEE 802 - Committee - LAN
- IEEE 802.11 - Committee - WLAN
  - Develop a protocols and transmission specifications for WLANs
- WECA - Wireless Ethernet Compatibility Alliance
  - Industry Consortium

802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

2. IEEE 802 Protocol Architecture

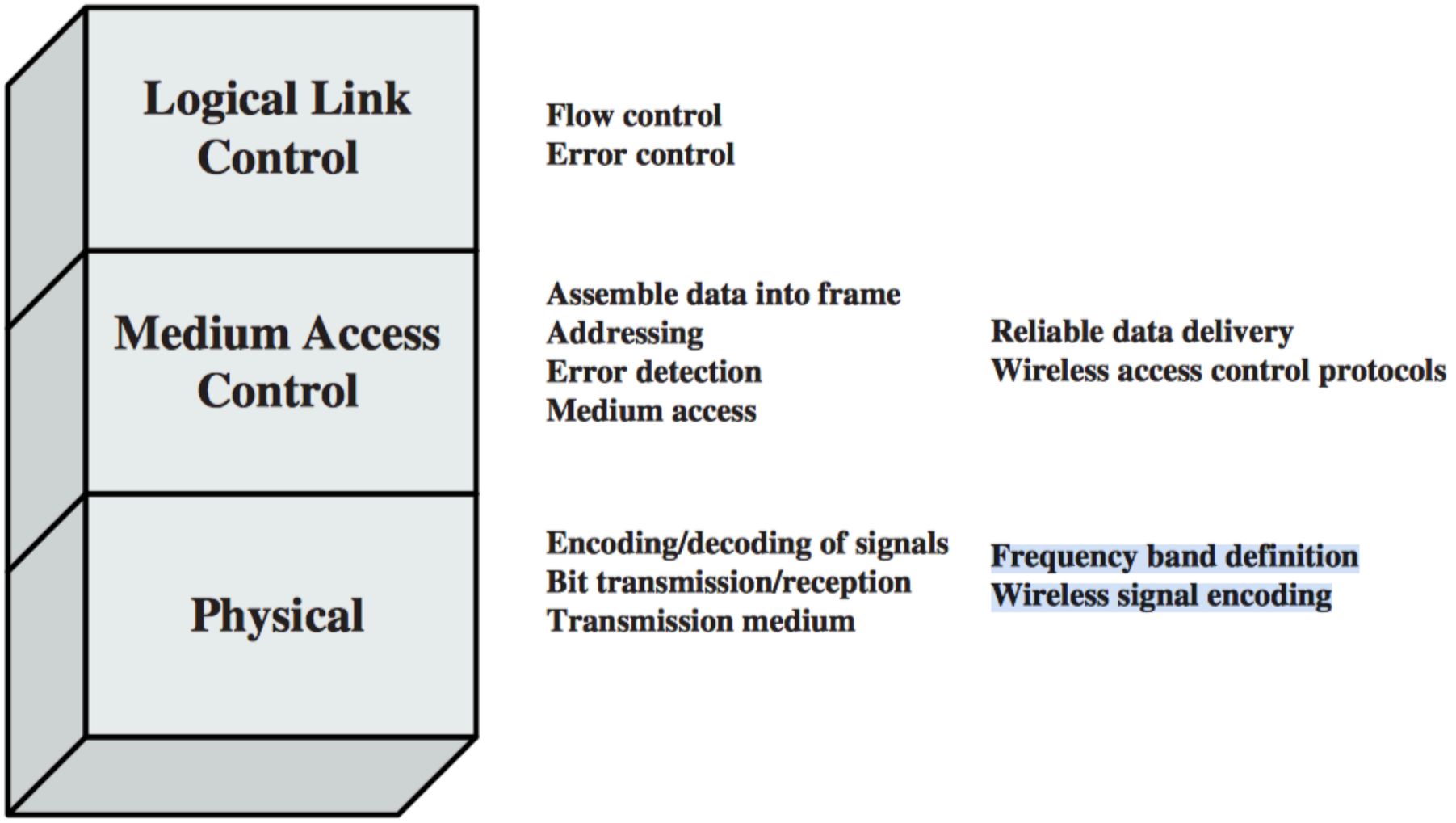


Figure 17.1 IEEE 802.11 Protocol Stack

2. IEEE 802 Protocol Architecture

1. Logical Link Control
2. Media Access Control
3. Physical Layer

1. Logical Link Control

- Flow Control
- Error Control

2. Media Access Control

- Assemble data into frame (MSDU -> MPDU)
- Addressing
- Error detection
- Medium access
- Specific IEEE 802.11 functions
  - Reliable data delivery
  - Wireless access control protocols

MPDU - MAC Protocol Data Unit
MSDU - MAC Service Data Unit

3.Physical Layer

- General IEEE 802 functions
  - Encoding/decoding of signals
  - Bit transmission/reception
  - Specification of Transmission medium
- Specific IEEE 802.11 functions
  - Frequency band definition
  - Wireless signal encoding

MPDU Frame Format

- Header
  - MAC Control
  - Dest. MAC Address
  - Source MAC Address
- Body
  - MSCU (Mac Service Data Unit)
- Trailer
  - CRC (Cyclic Redundancy Check) /FCS(Frame Check Sequence) Field

MPDU Frame Format

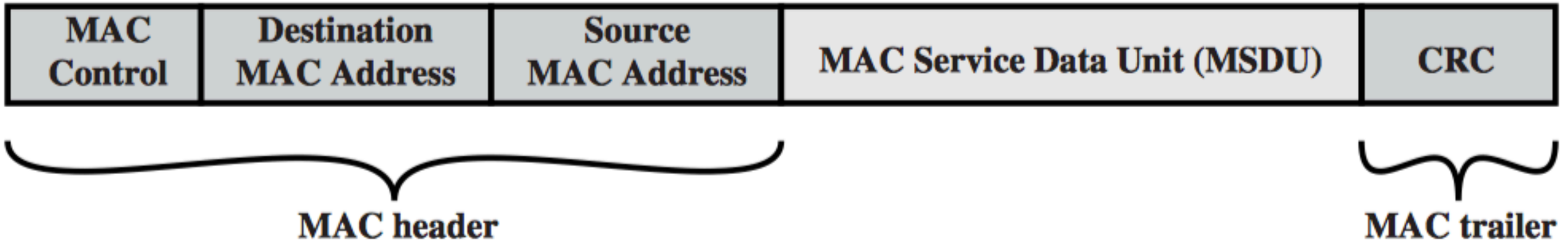


Figure 17.2 General IEEE 802 MPDU Format

3. IEEE 802.11 Network Components and Architectural Model

3. IEEE 802.11 Network Components and Architectural Model

- BSS - Basic Service Set
- DS - Distribution System
- AP - Access Point
- IBSS - Independent BSS
- ESS - Extended Service Set

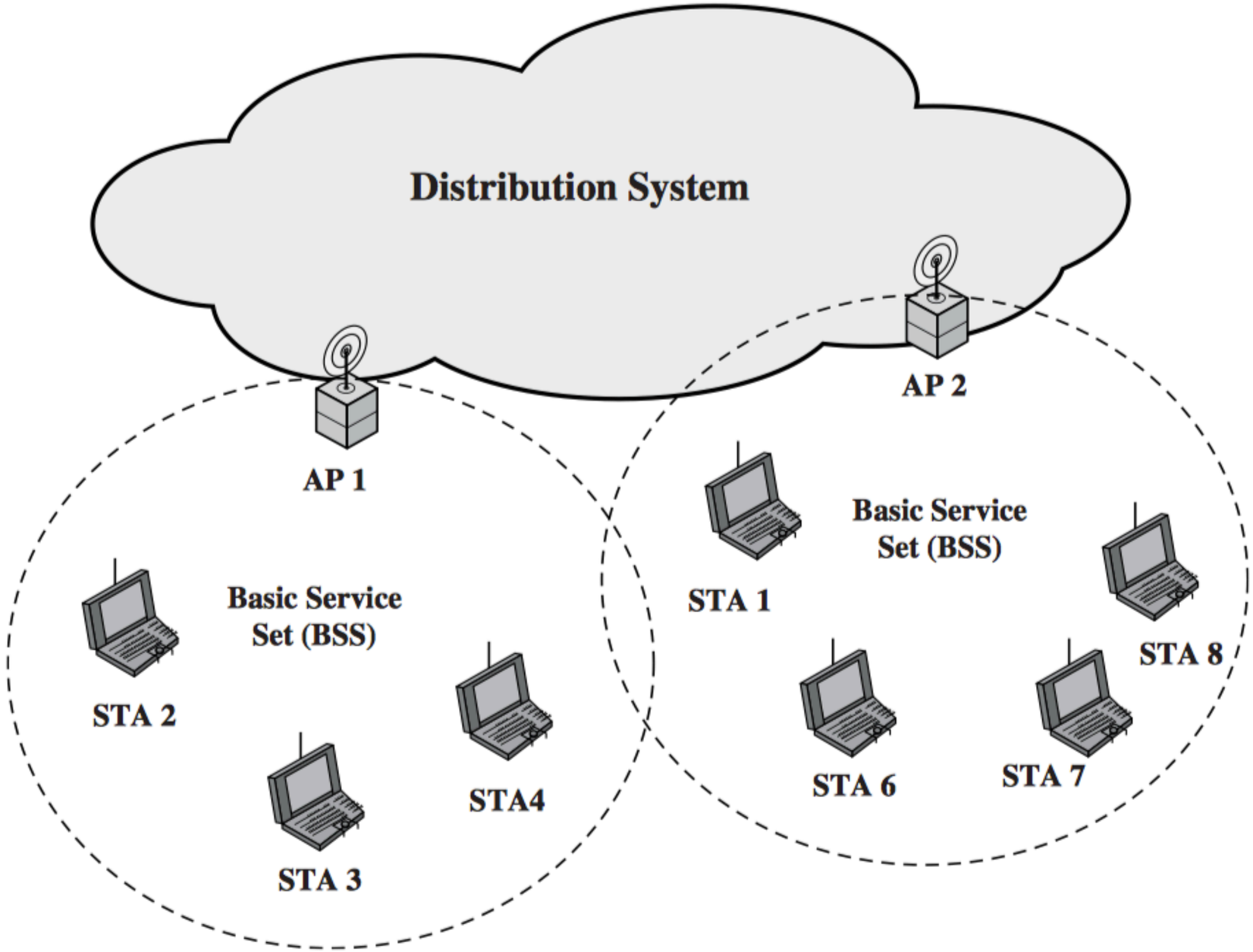


Figure 17.3 IEEE 802.11 Extended Service Set

Basic service set (BSS)

The smallest building block of a wireless LAN, which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.

A BSS may be isolated, or it may connect to a backbone **Distribution system (DS)** through an access point (AP).The AP functions as a bridge and a relay point.

When all the stations in the BSS are mobile stations that communicate directly with one another (not using an AP), the BSS is called an independent BSS (IBSS). An IBSS is typically an ad hoc network.

IEEE 802.11 Service

IEEE 802.11 Service

- Services that needs to be provided by the wireless LAN to achieve the functionality equivalent to that which is inherent to wired LAN.

Table 17.2 IEEE 802.11 Services

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

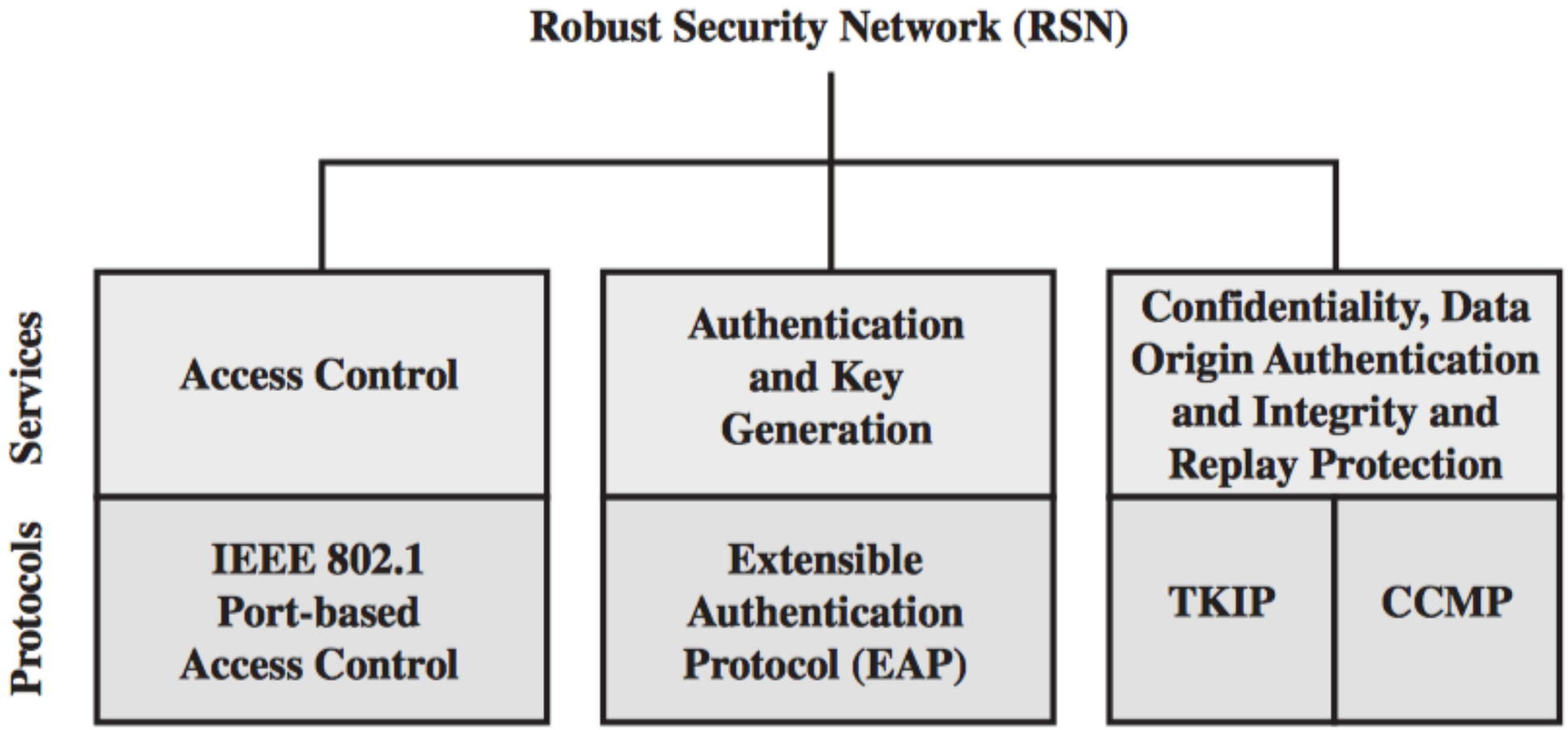
Categeorization of Service

- Based on Provider
  - DS - Distribution System
  - SS - Service Station
- Based on the Nature of Service
  - LAN Access
  - MSDU Delivery

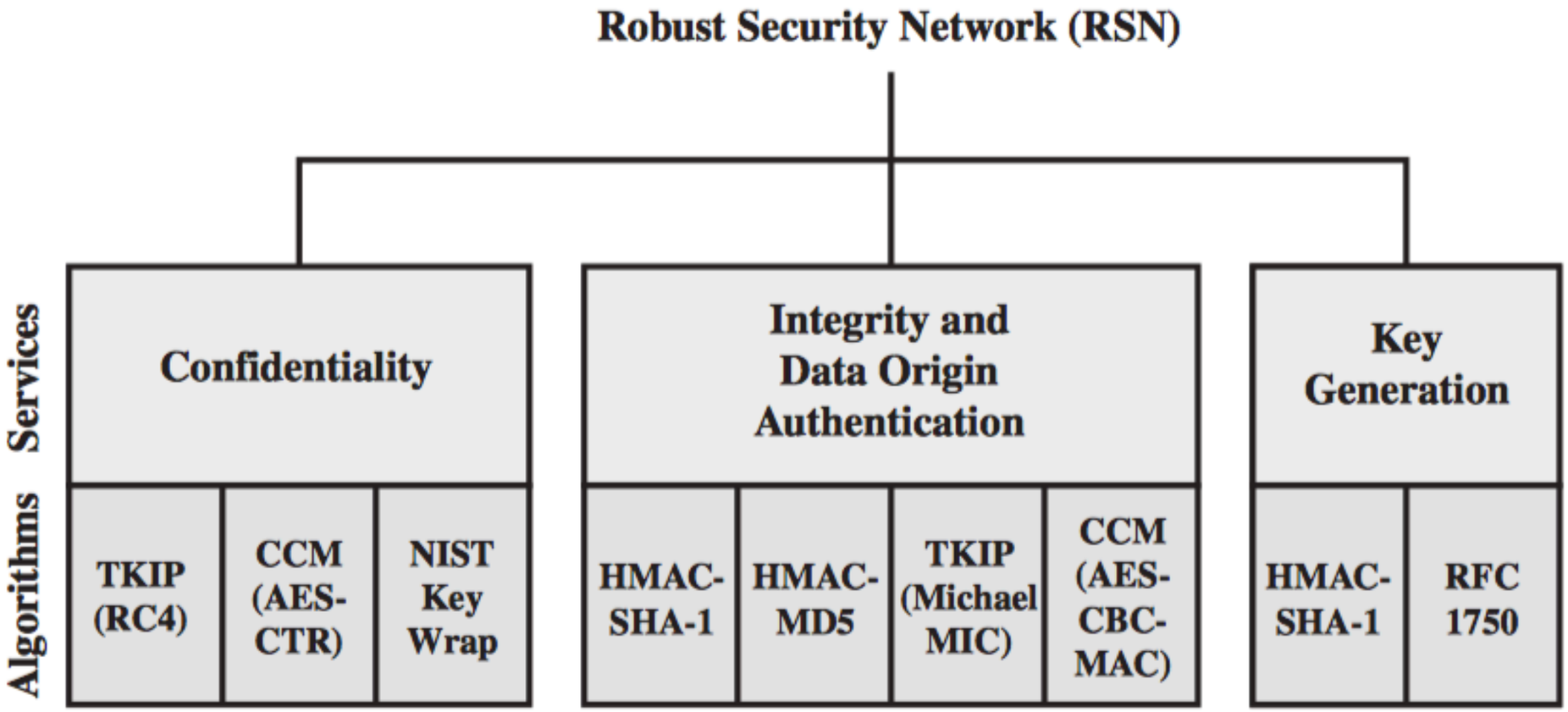
- Distribution of Messages within a DS
- Association related services
  - 3 Transition types
    - No Transition
    - BSS Transition
    - ESS Transition
  - 3 Services
    - Association
    - Reassociation
    - Disassociation

Table 17.3 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) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 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) 128 (CCMP) 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



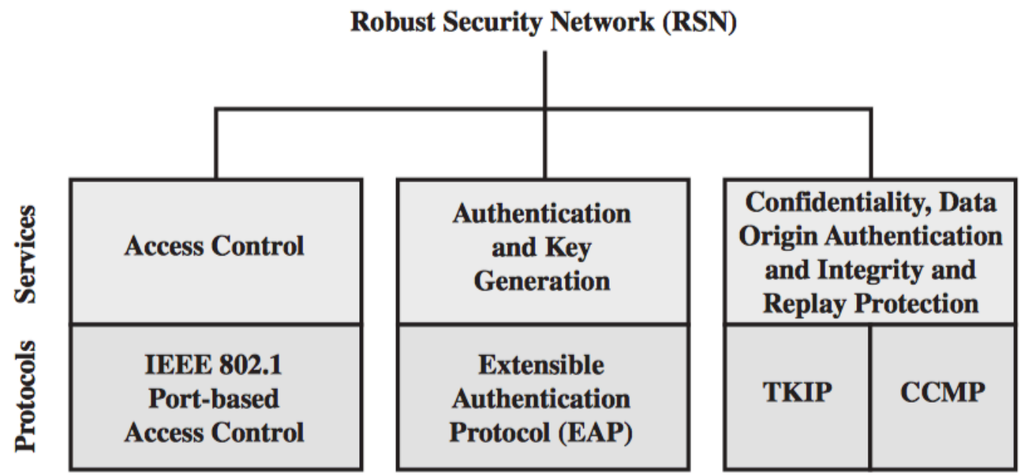
(a) Services and protocols



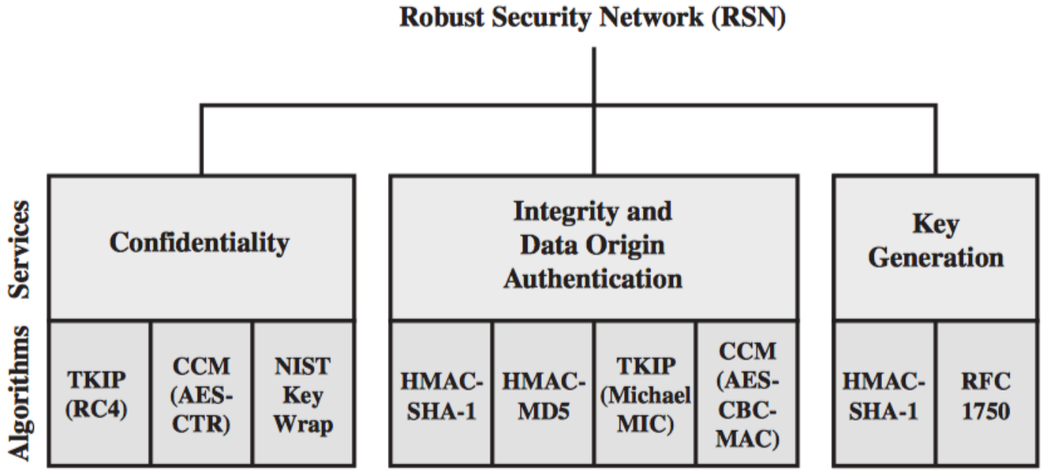
(b) Cryptographic algorithms

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 17.4 Elements of IEEE 802.11i



(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 17.4 Elements of IEEE 802.11i

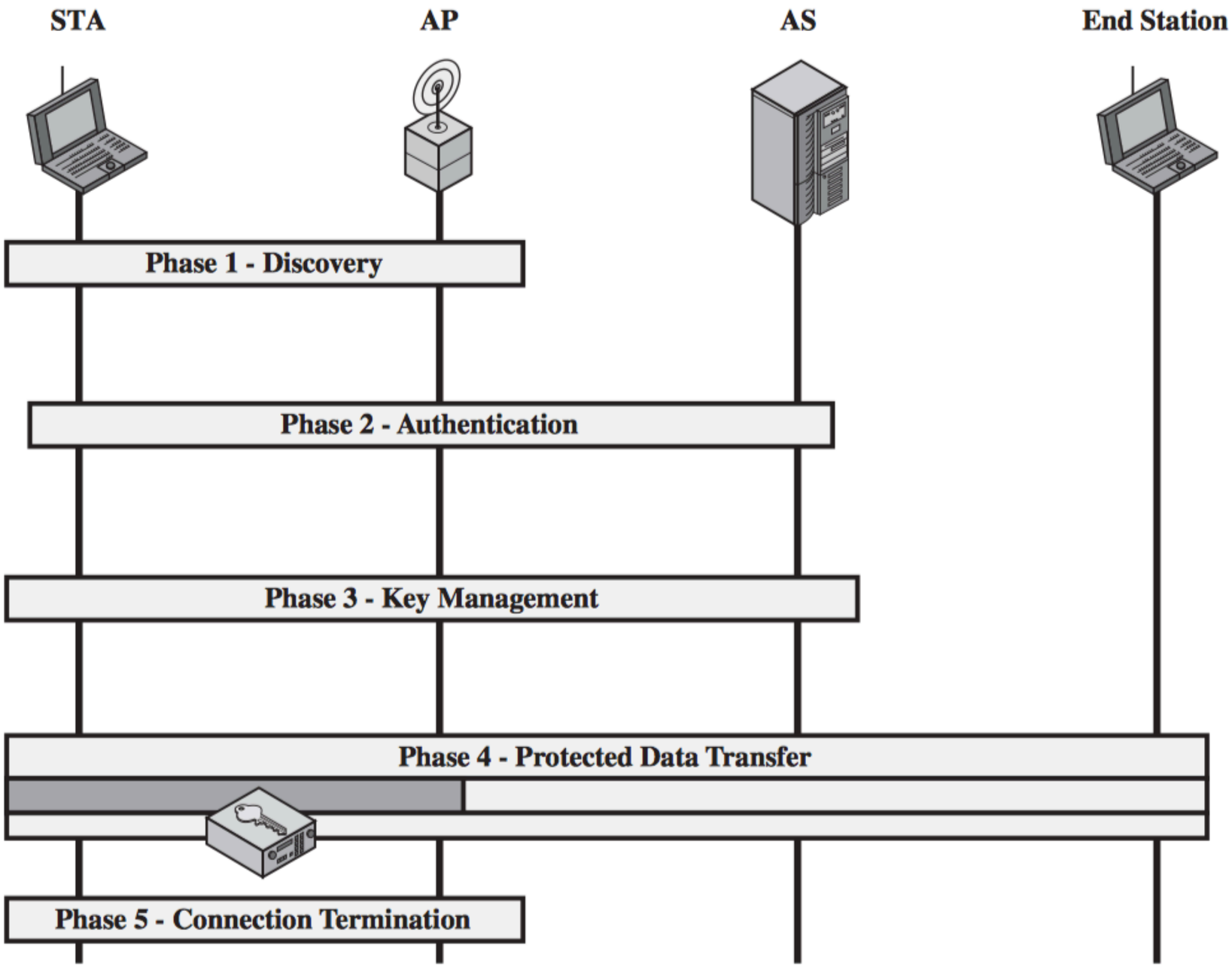


Figure 17.5 IEEE 802.11i Phases of Operation

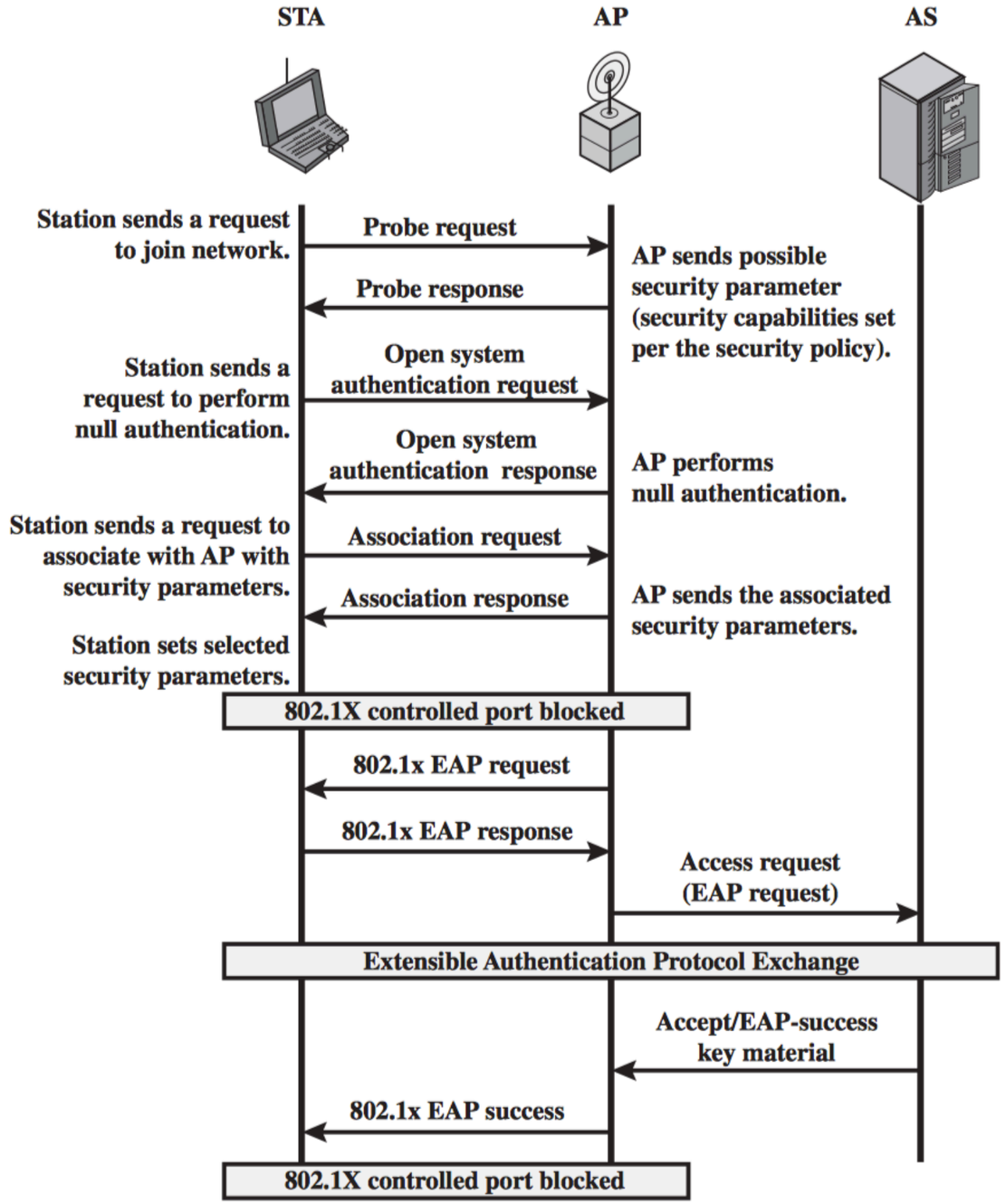


Figure 17.6 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

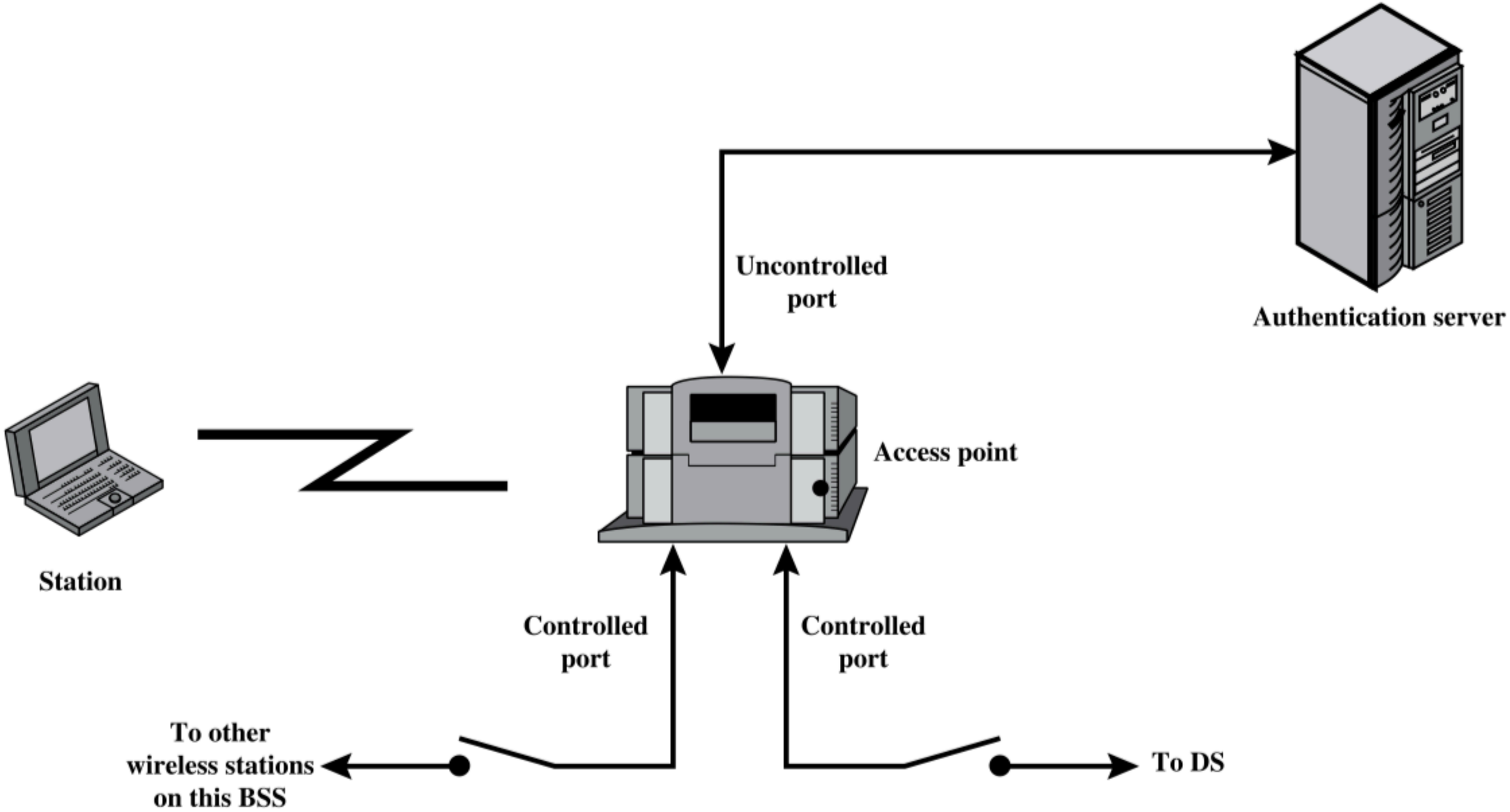
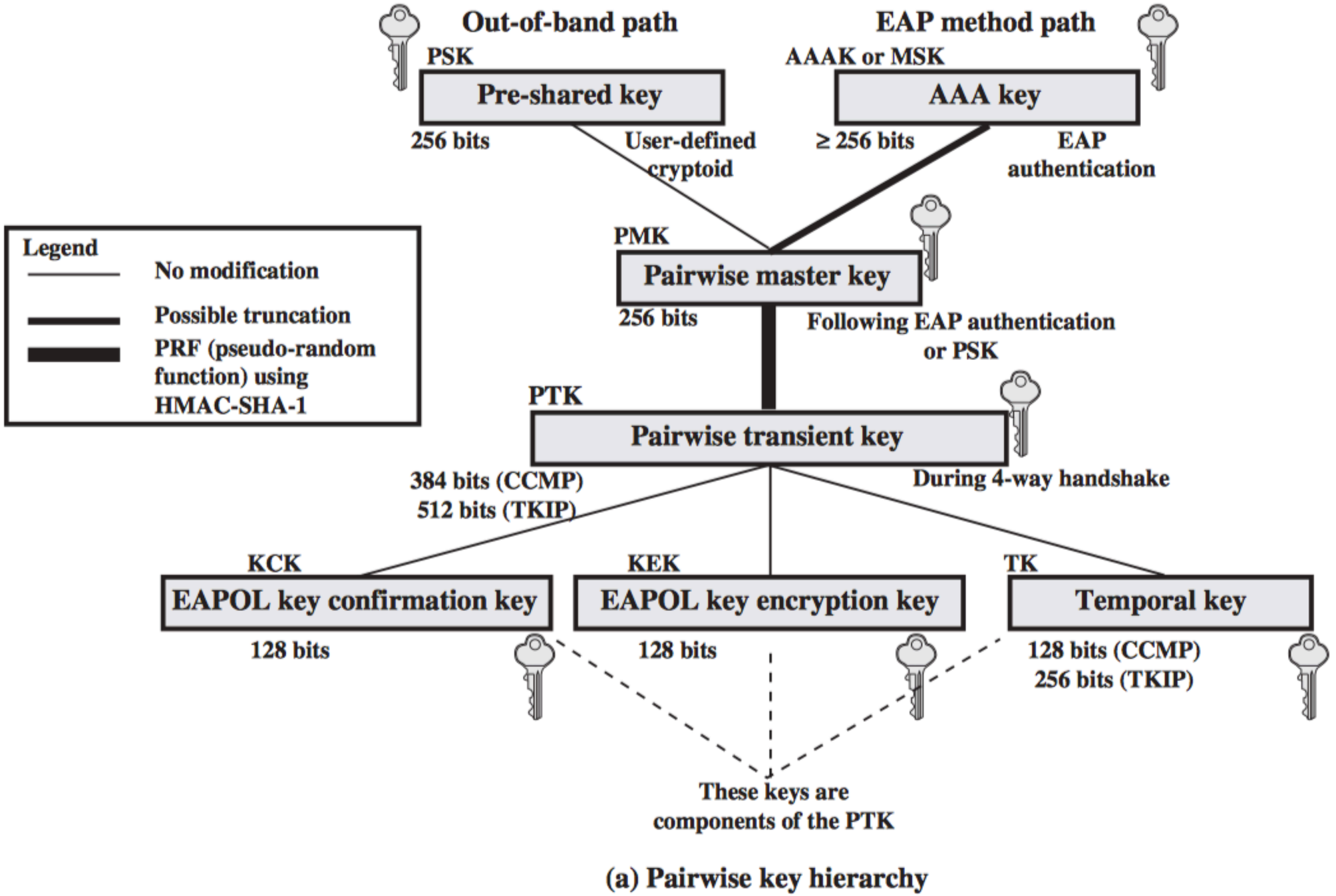


Figure 17.7 802.1X Access Control



(a) Pairwise key hierarchy

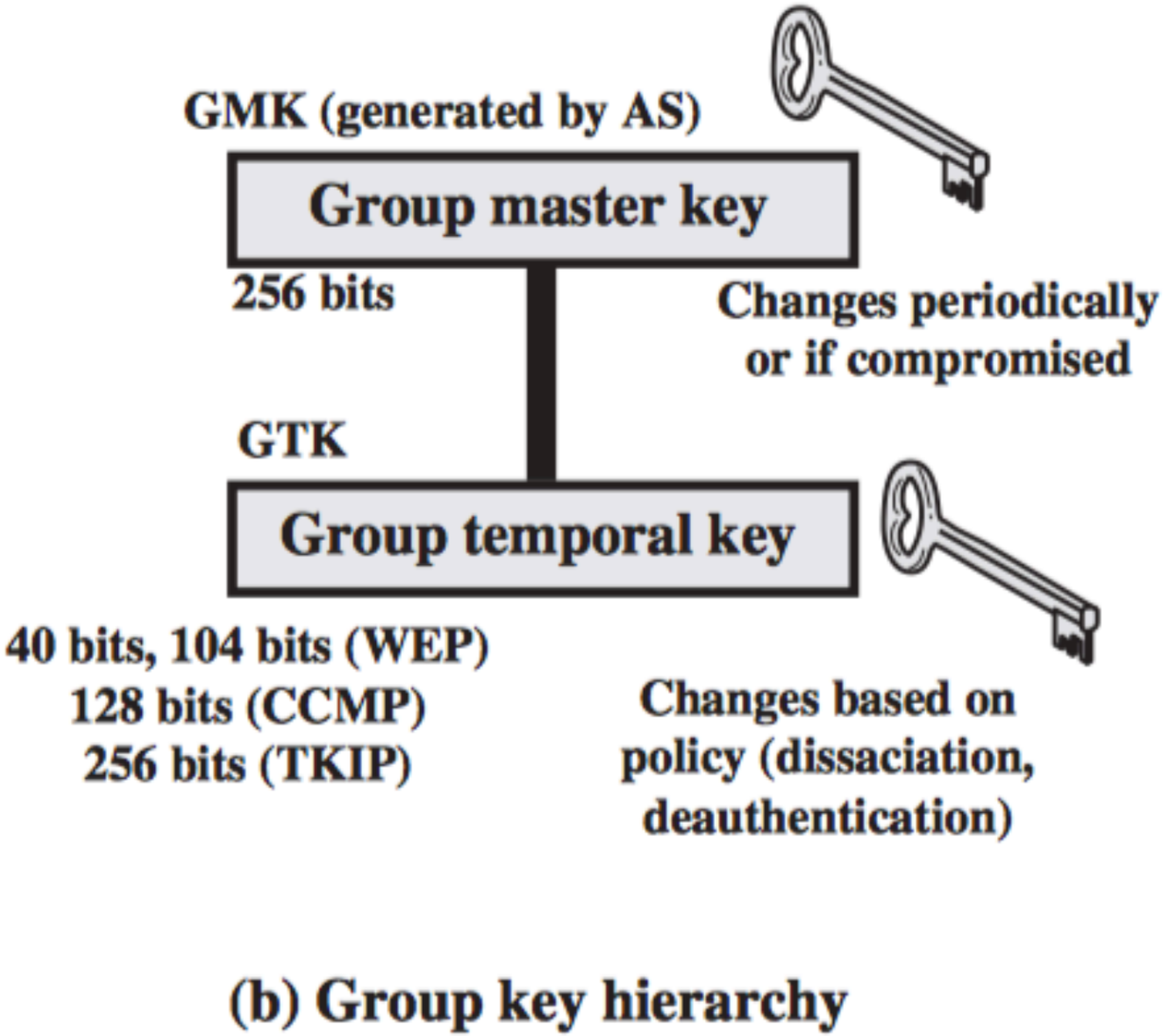


Figure 17.8 IEEE 802.11i Key Hierarchies

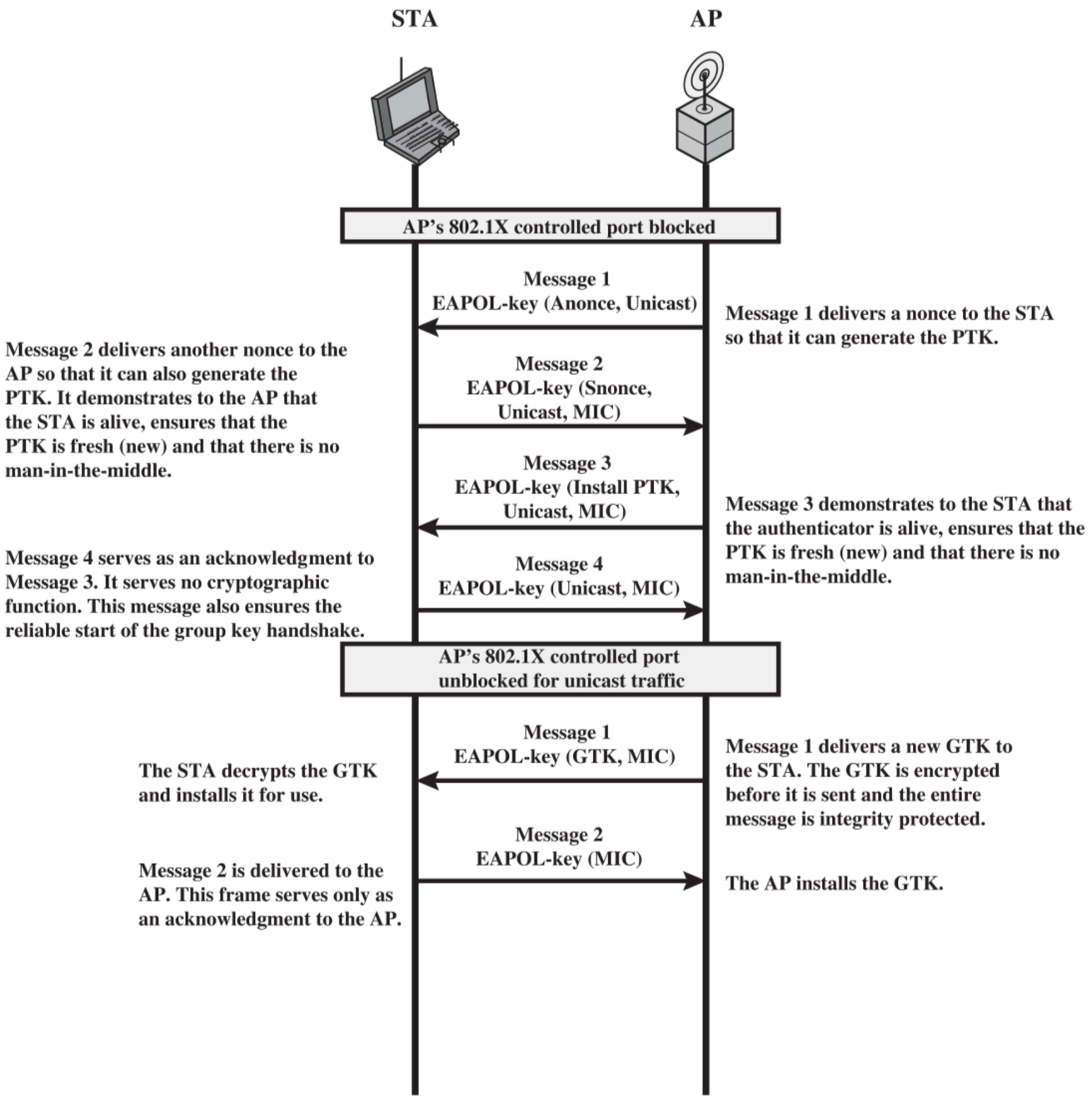
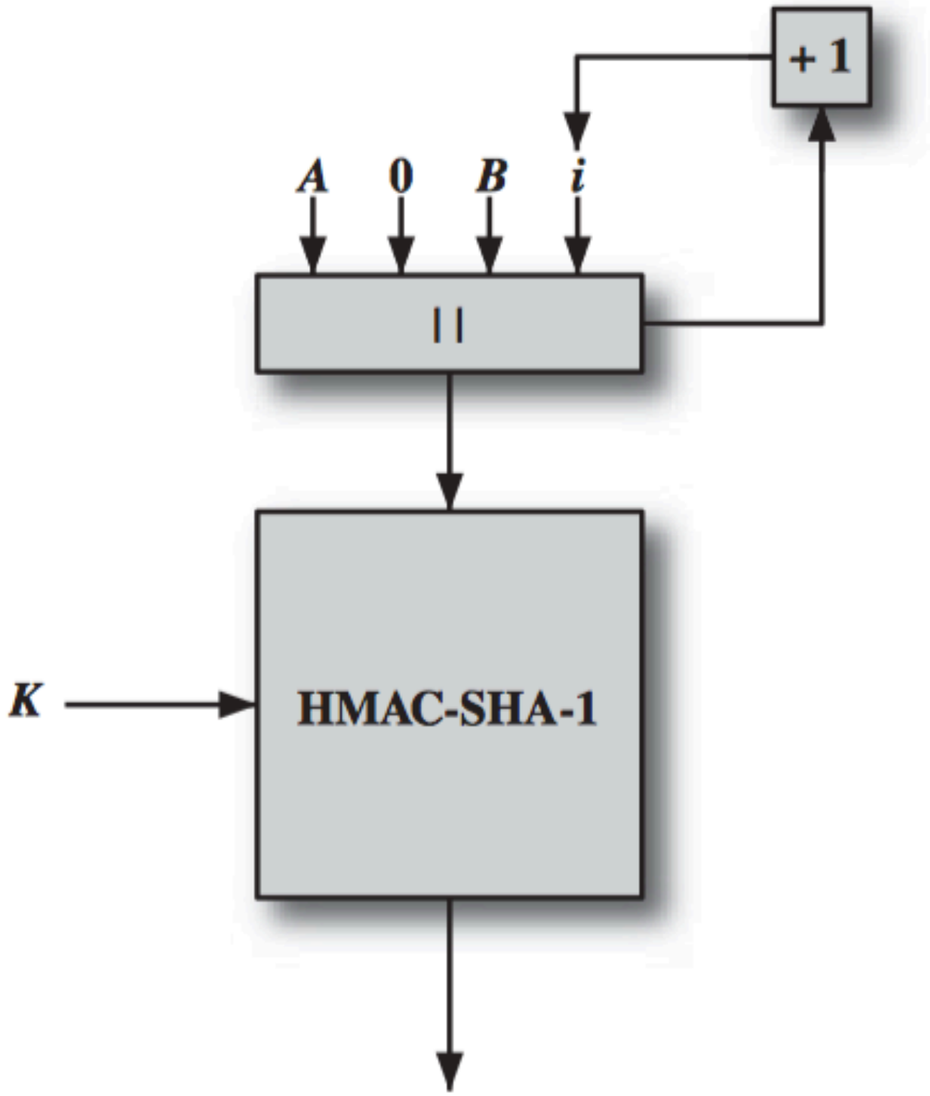


Figure 17.9 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake



$$R = \text{HMAC-SHA-1}(K, A \parallel 0 \parallel B \parallel i)$$

Figure 17.10 IEEE 802.11i Pseudorandom Function

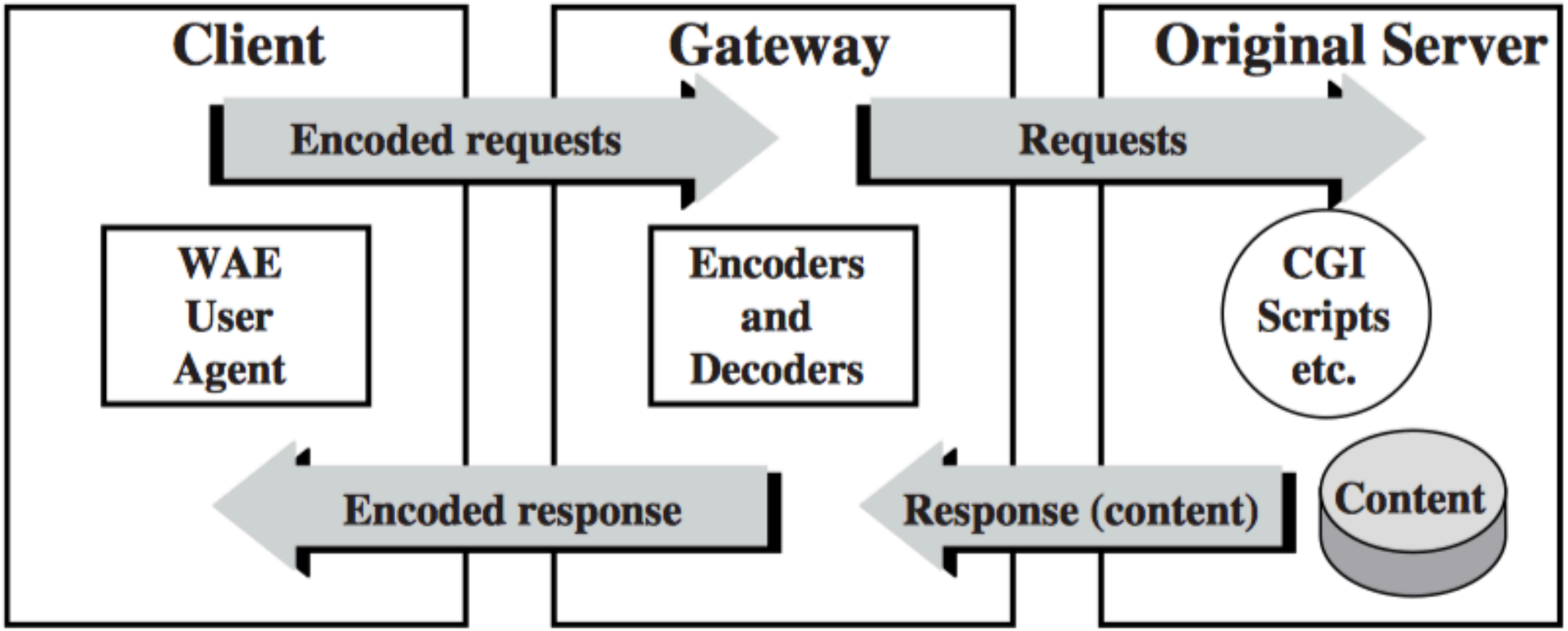


Figure 17.11 The WAP Programming Model

WAP

Wireless Application Protocol

History

- Introduced in 1999
- Used widely in early 2000s
- By 2010 use of WAP Declined

WAP Key points

- WAP used WML (wireless markup language)

WAP Protocol Stack

Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Wireless Datagram Protocol (WDP)

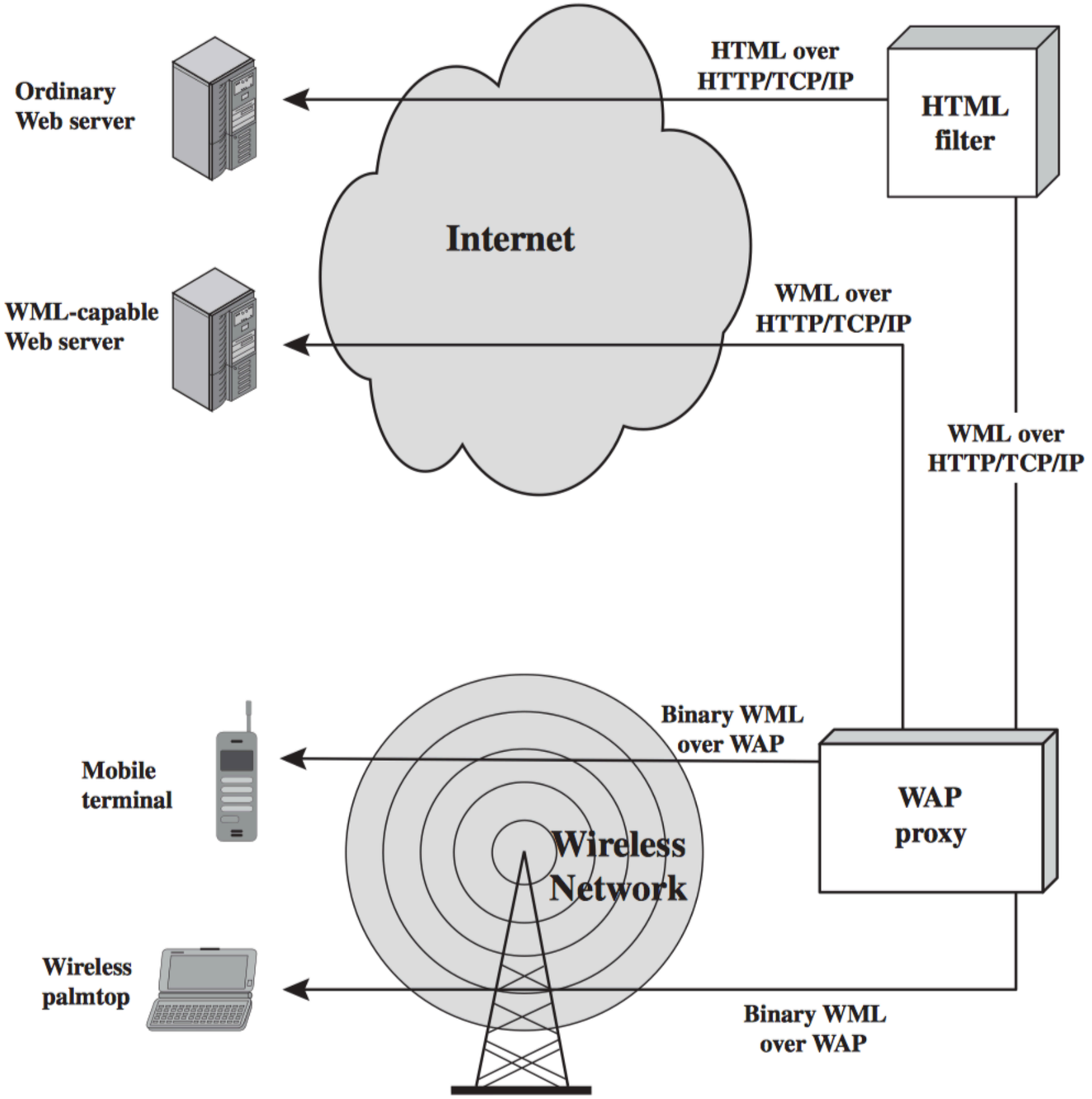


Figure 17.12 WAP Infrastructure

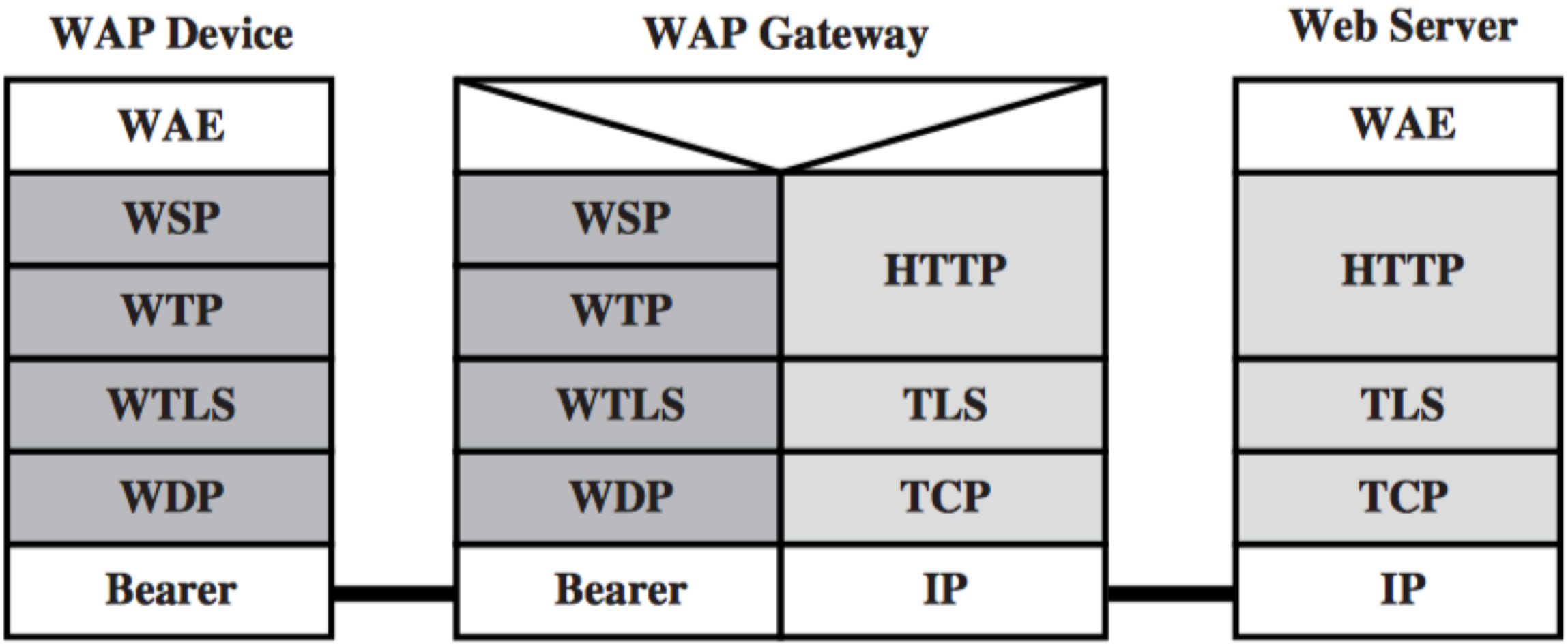


Figure 17.14 WTP 1.x Gateway

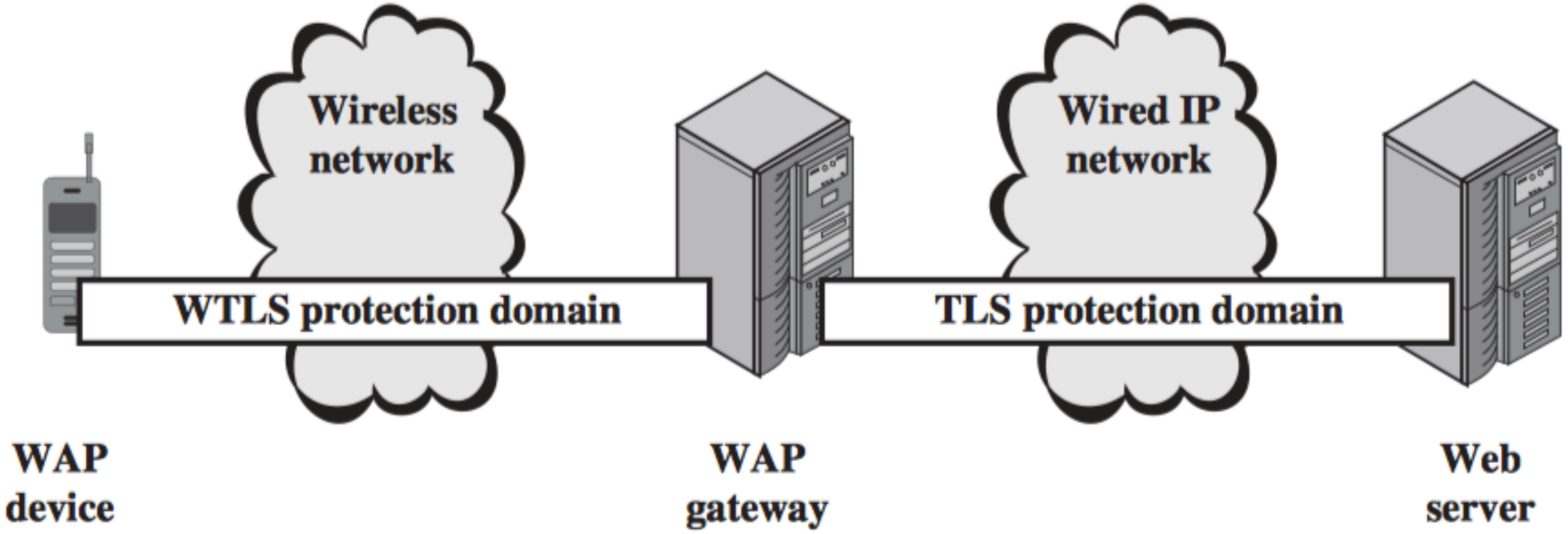
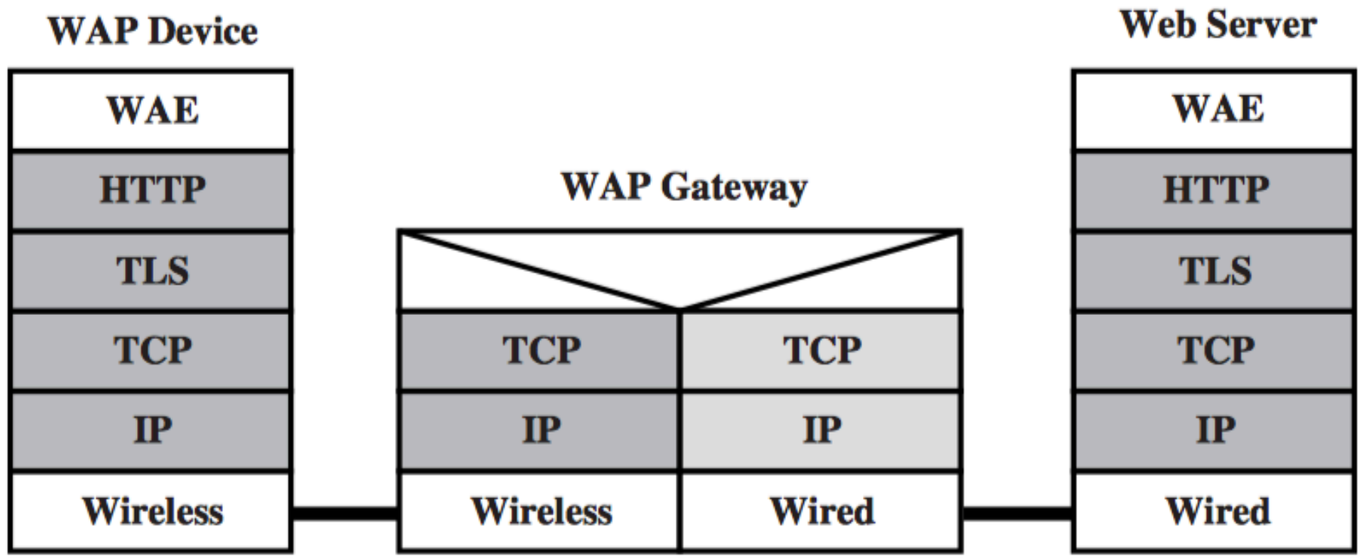
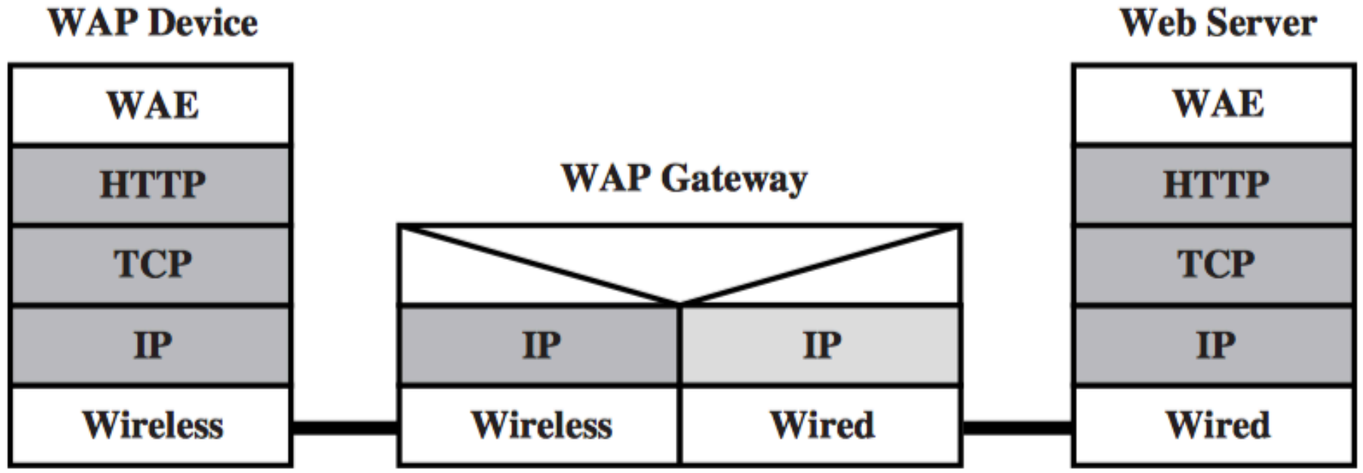


Figure 17.19 Security Zones Using Standard Security Services



(a) TLS-based security



(b) IPSec-based security

Figure 17.20 WAP2 End-to-End Security Approaches