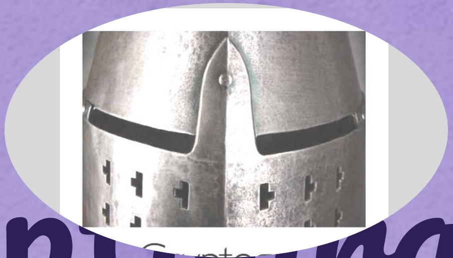


Cryptography and Network Security

Sixth Edition

by William Stallings

Chapter 18

Wireless Network Security

“Investigators have published numerous reports of birds taking turns vocalizing; the bird spoken to gave its full attention to the speaker and never vocalized at the same time, as if the two were holding a conversation.”

“Researchers and scholars who have studied the data on avian communication carefully write (a) the communication code of birds, such as crows, has not been broken by any means; (b) probably all birds have wider vocabularies than anyone realizes; and (c) greater complexity and depth are recognized in avian communication as research progresses.”

—The Human Nature of Birds,
Theodore Barber

Wireless Security

- Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include:

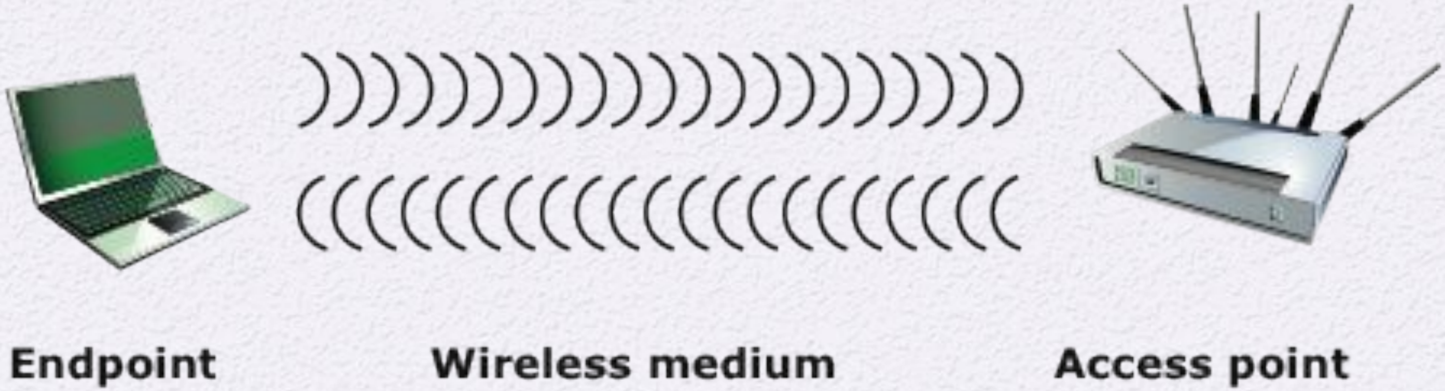


Figure 18.1 Wireless Networking Components

Wireless Network Threats

- **Accidental association**
  - Company wireless LANs in close proximity may create overlapping transmission ranges
  - A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network
- **Malicious association**
  - In this situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point
- **Ad hoc networks**
  - These are peer-to-peer networks between wireless computers with no access point between them
  - Such networks can pose a security threat due to a lack of a central point of control
- **Nontraditional networks**
  - Personal network Bluetooth devices, barcode readers, and handheld PDAs pose a security risk in terms of both eavesdropping and spoofing
- **Identity theft (MAC spoofing)**
  - This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges
- **Man-in-the-middle attacks**
  - This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device
  - Wireless networks are particularly vulnerable to such attacks
- **Denial of service (DoS)**
  - This attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources
  - The wireless environment lends itself to this type of attack because it is so easy for the attacker to direct multiple wireless messages at the target
- **Network injection**
  - This attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages

Securing Wireless Transmissions

- The principal threats to wireless transmission are eavesdropping, altering or inserting messages, and disruption

- To deal with eavesdropping, two types of countermeasures are appropriate:
  - Signal-hiding techniques
    - Turn off SSID broadcasting by wireless access points
    - Assign cryptic names to SSIDs
    - Reduce signal strength to the lowest level that still provides requisite coverage
    - Locate wireless access points in the interior of the building, away from windows and exterior walls
  - Encryption
    - Is effective against eavesdropping to the extent that the encryption keys are secured

Securing Wireless Access Points

- The main threat involving wireless access points is unauthorized access to the network
- The principal approach for preventing such access is the IEEE 802.1x standard for port-based network access control
  - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
  - The use of 802.1x can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

Securing Wireless Networks

Mobile Device Security

- Mobile devices have become an essential element for organizations as part of the overall network infrastructure
- Prior to the widespread use of smartphones, network security was based upon clearly defined perimeters that separated trusted internal networks from the untrusted Internet
- Due to massive changes, an organization's networks must now accommodate:
  - Growing use of new devices
  - Cloud-based applications
  - De-perimeterization
  - External business requirements

Security Threats

- Major security concerns for mobile devices:

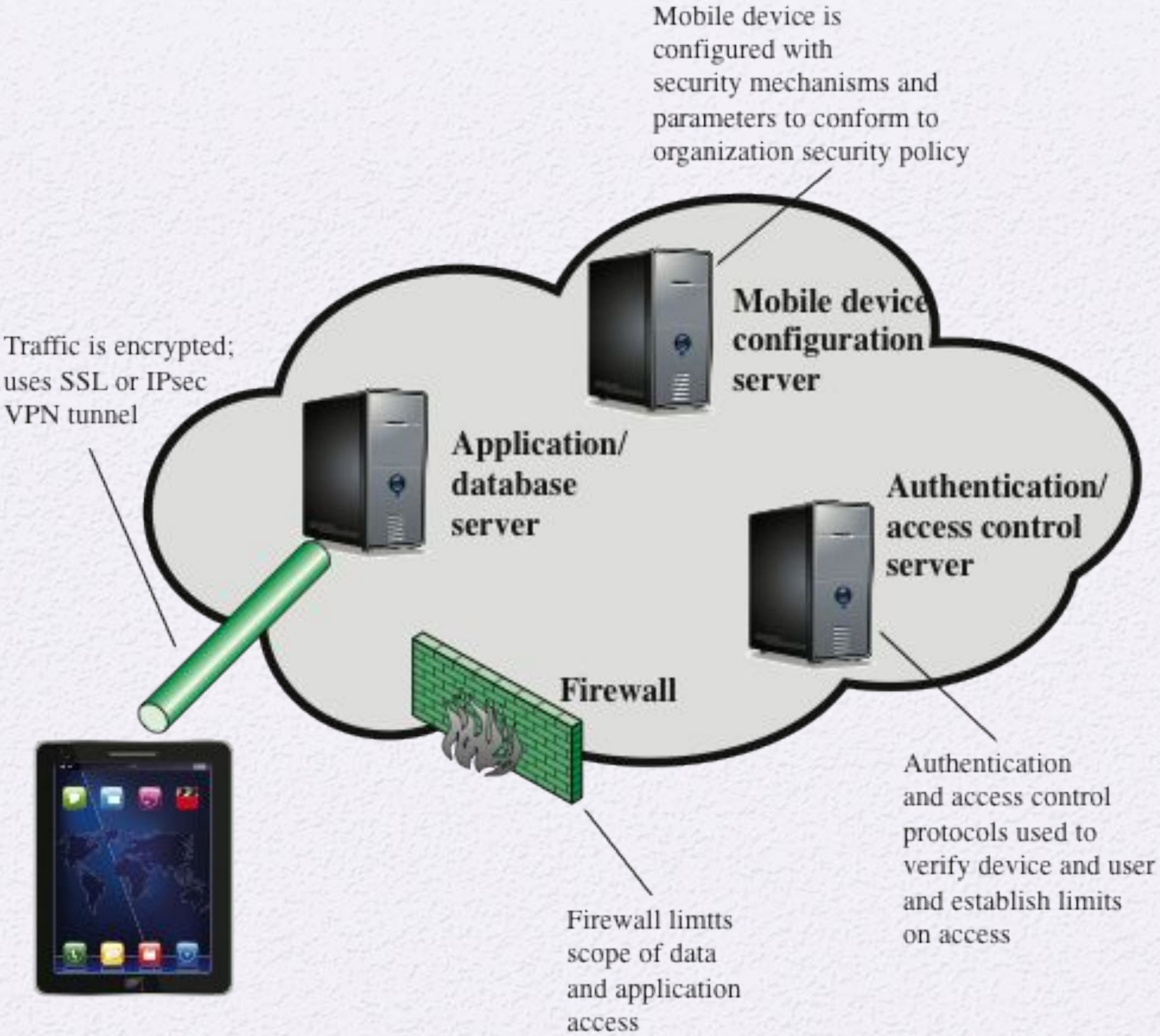
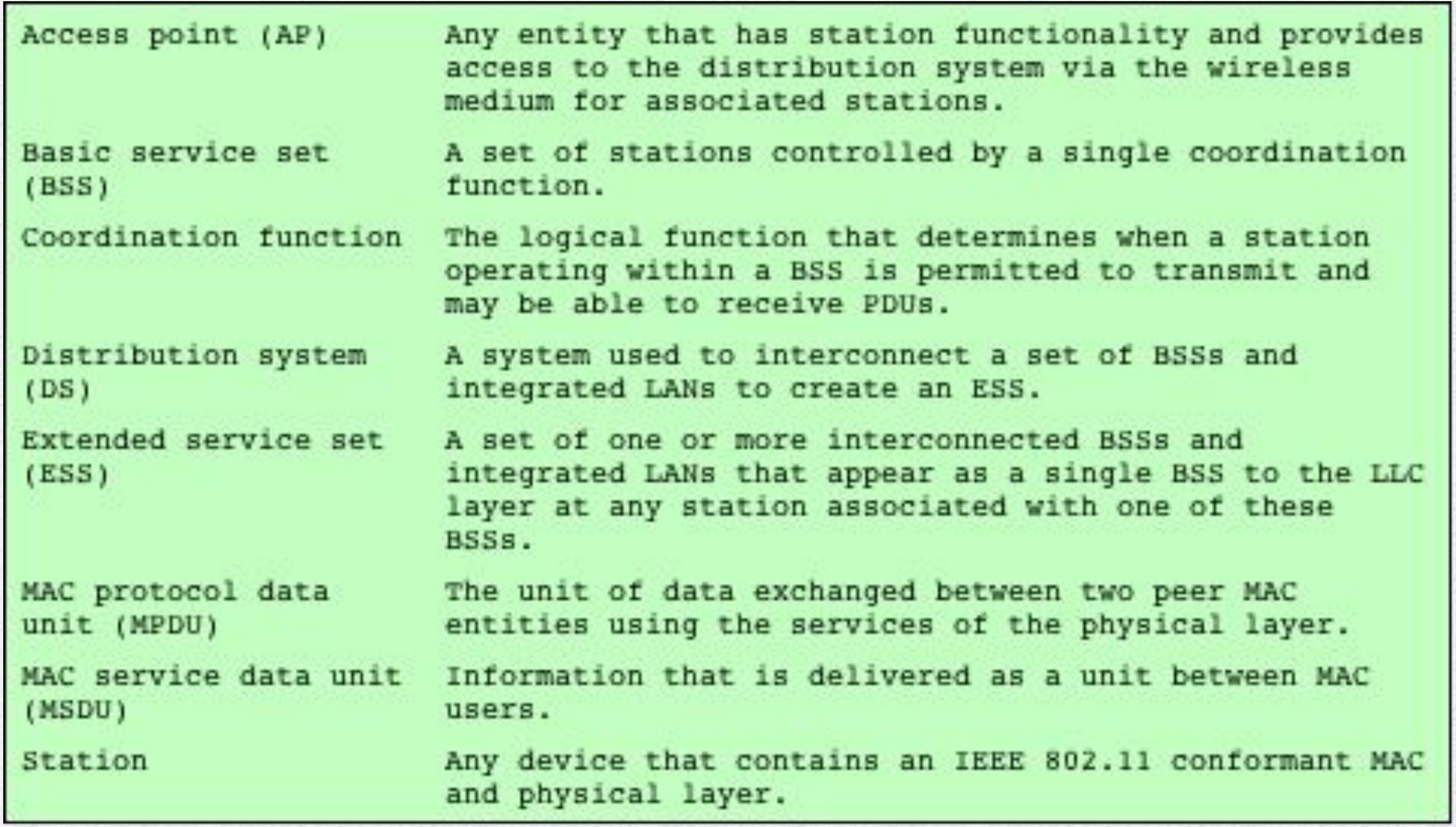

Mobile device is configured with security mechanisms and parameters to conform to organization security policy
Mobile device configuration server
Traffic is encrypted; uses SSL or IPsec VPN tunnel
Application/ database server
Authentication/ access control server
Firewall
Authentication and access control protocols used to verify device and user and establish limits on access
Firewall limtts scope of data and application access

Figure 18.2 Mobile Device Security Elements

IEEE 802.11
Wireless LAN Overview

- IEEE 802 is a committee that has developed standards for a wide range of local area networks (LANs)
- In 1990 the IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs)
- Since that time, the demand for WLANs at different frequencies and data rates has exploded

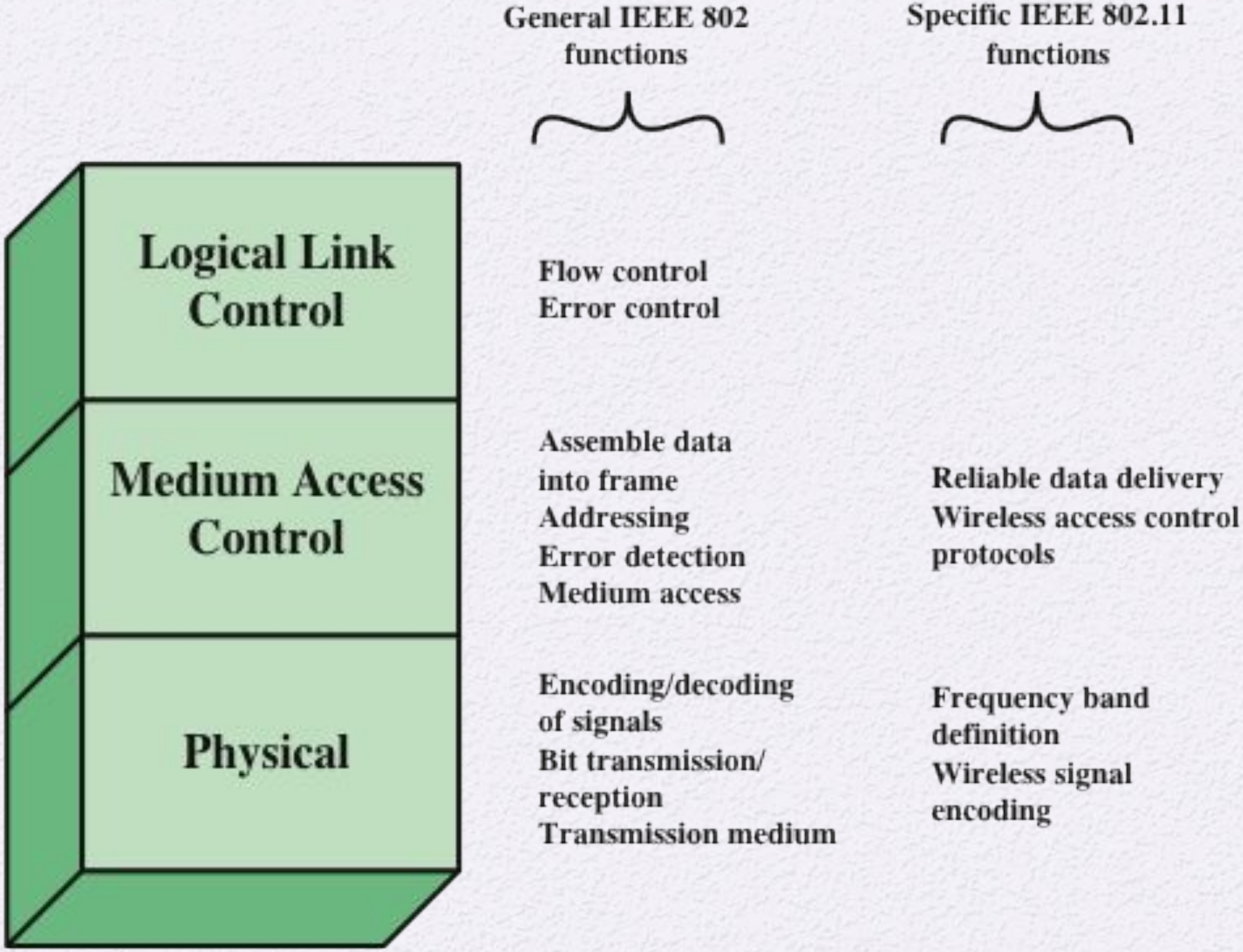
Table 18.1
IEEE 802.11 Terminology



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.

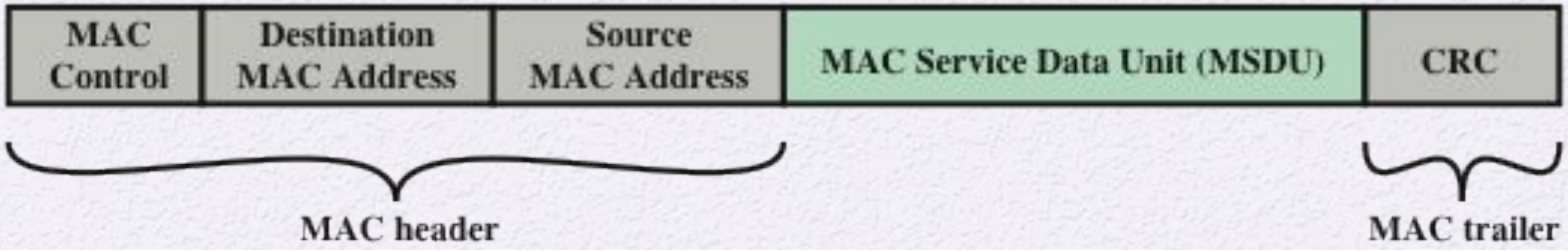
Wi-Fi Alliance

- The first 802.11 standard to gain broad industry acceptance was 802.11b
- Wireless Ethernet Compatibility Alliance (WECA)
  - An industry consortium formed in 1999
  - Subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance
  - Created a test suite to certify interoperability for 802.11 products
- Wi-Fi
  - The term used for certified 802.11b products
  - Has been extended to 802.11g products
- Wi-Fi5
  - A certification process for 802.11a products that was developed by the Wi-Fi Alliance
- Recently the Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards
  - Referred to as Wi-Fi Protected Access (WPA)



	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow control Error control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocols
Physical	Encoding/decoding of signals Bit transmission/ reception Transmission medium	Frequency band definition Wireless signal encoding

Figure 18.3 IEEE 802.11 Protocol Stack



MAC Control

Destination MAC Address

Source MAC Address

MAC Service Data Unit (MSDU)

CRC

MAC header

MAC trailer

Figure 18.4 General IEEE 802 MPDU Format

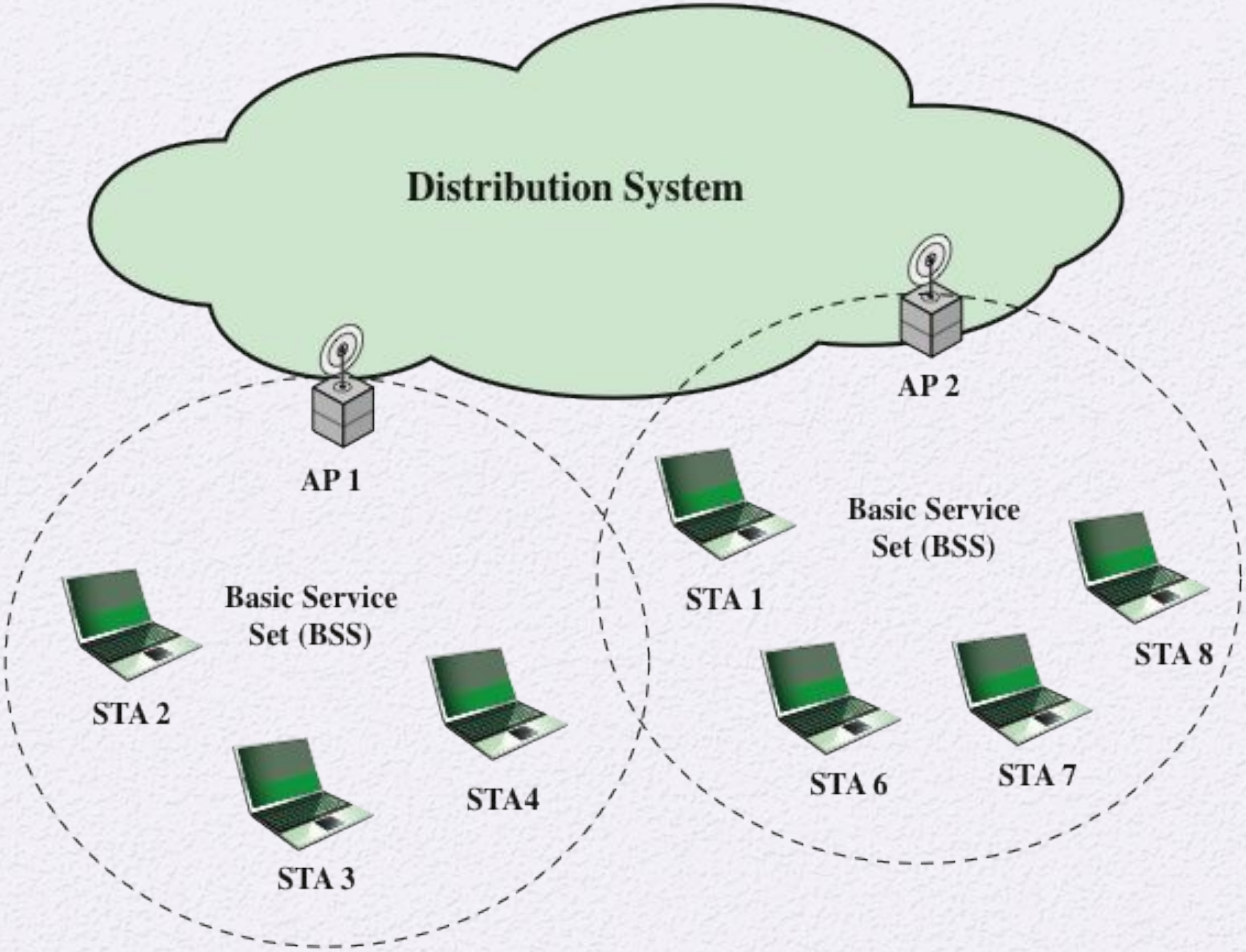
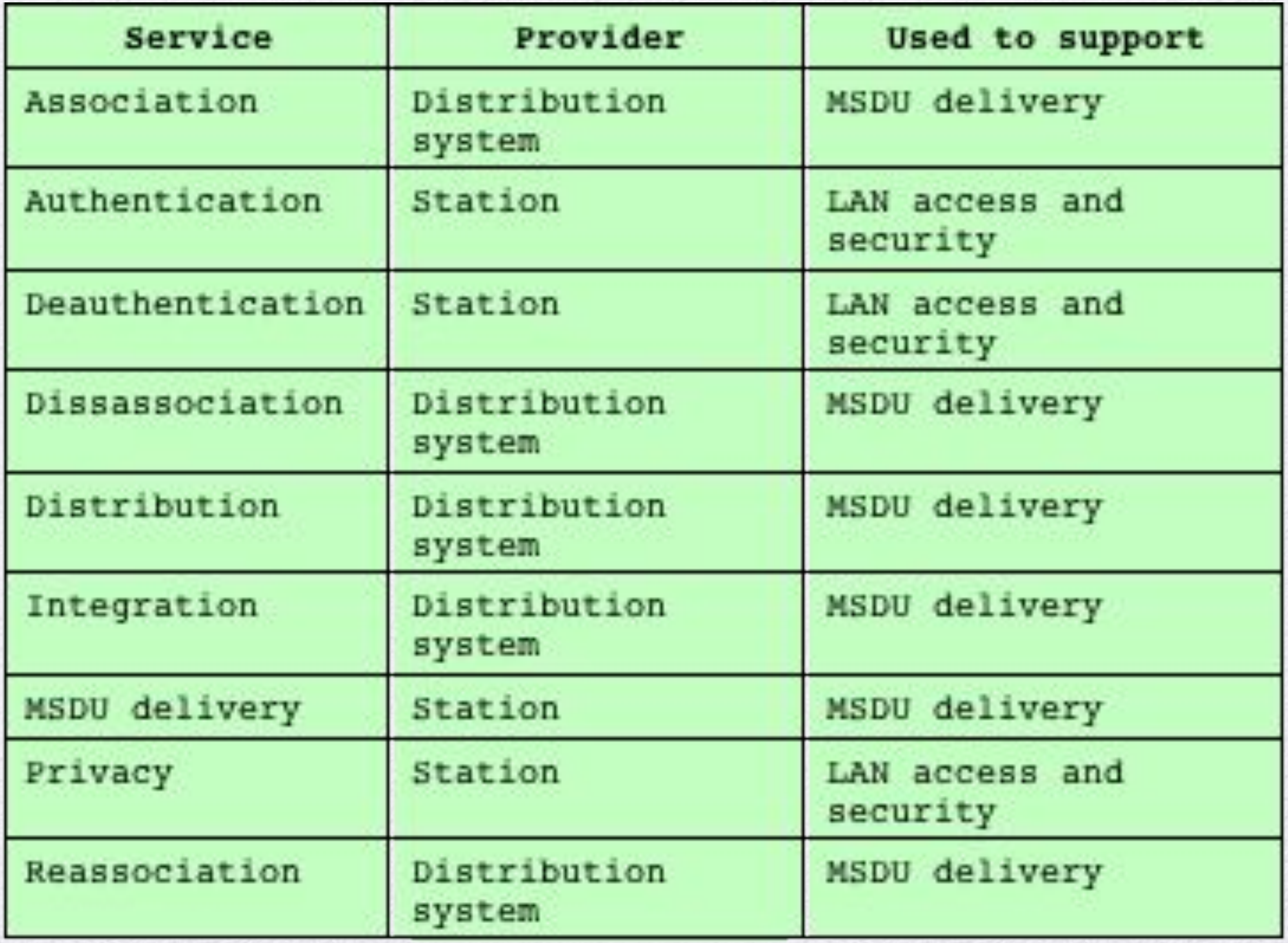


Figure 18.5 IEEE 802.11 Extended Service Set

Table 18.2
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
Dissassociation	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

Distribution of Messages Within a DS

- The two services involved with the distribution of messages within a DS are:

Association-Related Services

- Transition types based on mobility:

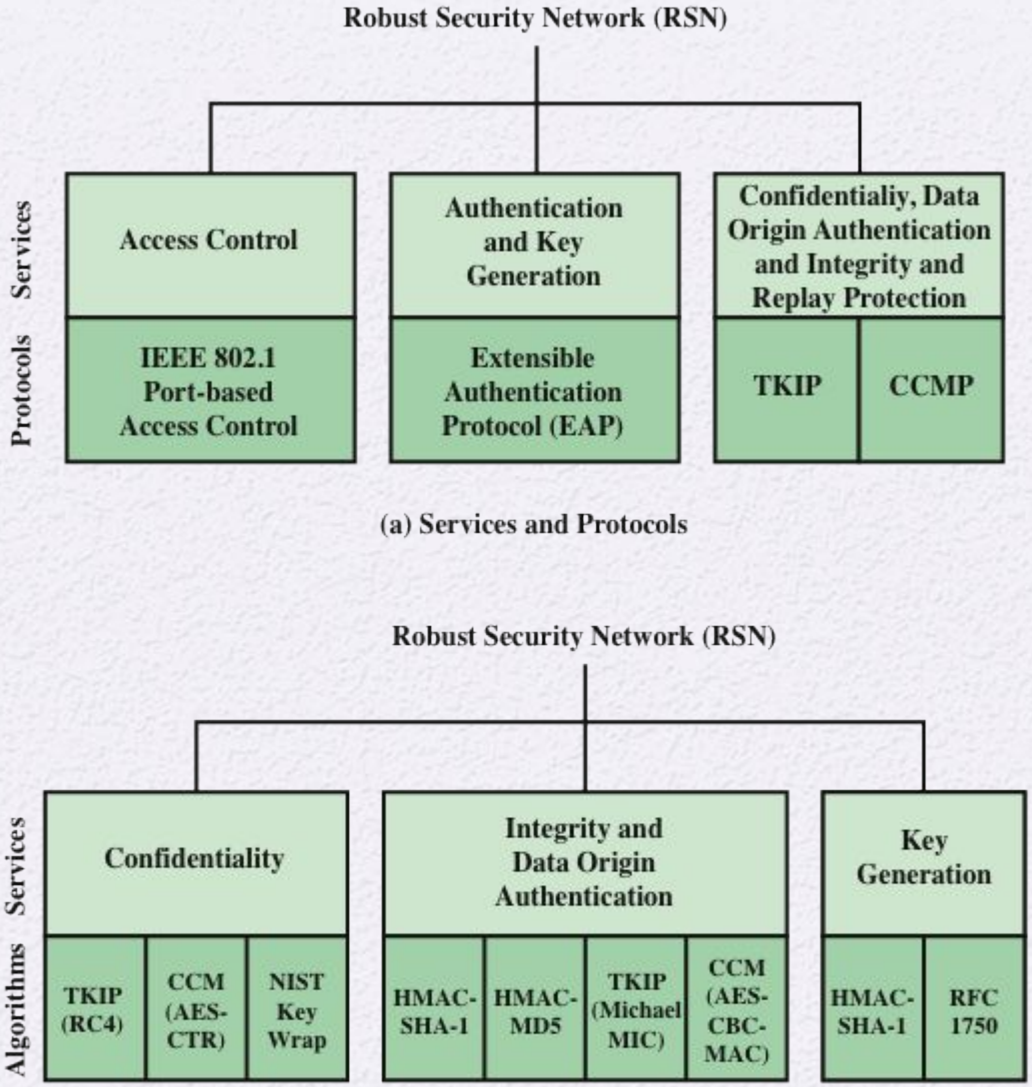
Association-Related Services

- To deliver a message within a DS, the distribution service needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station

- Three services relate to a station maintaining an association with the AP within its current BSS:
  - Association
    - Establishes an initial association between a station and an AP
  - Reassociation
    - Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another
  - Disassociation
    - A notification from either a station or an AP that an existing association is terminated

IEEE 802.11i Wireless LAN Security

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



Robust Security Network (RSN)

Services

Protocols

Access Control

IEEE 802.1
Port-based
Access Control

Authentication
and Key
Generation

Extensible
Authentication
Protocol (EAP)

Confidentialiy, Data
Origin Authentication
and Integrity and
Replay Protection

TKIP

CCMP

(a) Services and Protocols

Robust Security Network (RSN)

Services

Algorithms

Confidentiality

TKIP
(RC4)

CCM
(AES-
CTR)

NIST
Key
Wrap

Integrity and
Data Origin
Authentication

HMAC-
SHA-1

HMAC-
MD5

TKIP
(Michael
MIC)

CCM
(AES-
CBC-
MAC)

Key
Generation

HMAC-
SHA-1

RFC
1750

(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 18.6 Elements of IEEE 802.11i

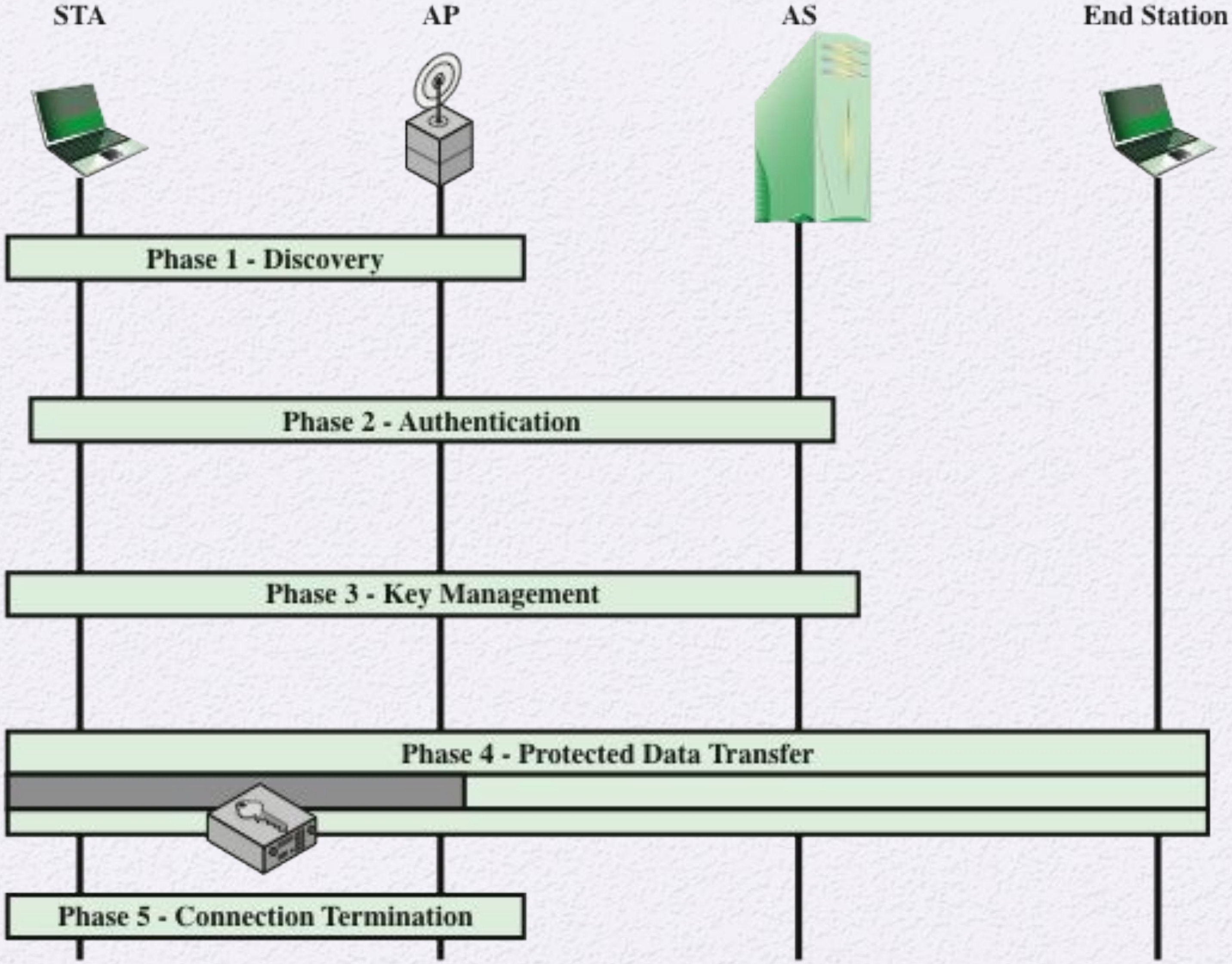


Figure 18.7 IEEE 802.11i Phases of Operation

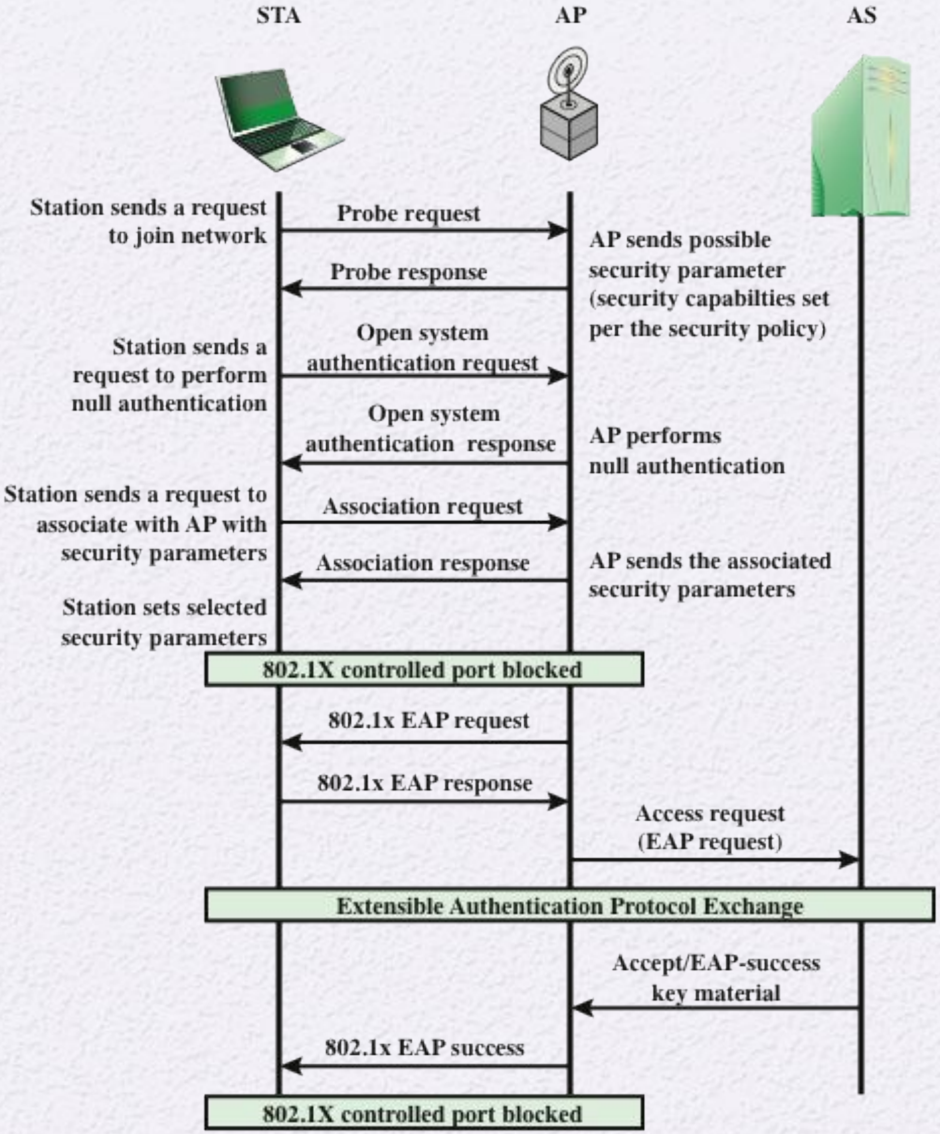

STA
AP
AS
Station sends a request to join network
Probe request
Probe response
AP sends possible security parameter (security capabilties set per the security policy)
Station sends a request to perform null authentication
Open system authentication request
Open system authentication response
AP performs null authentication
Station sends a request to associate with AP with security parameters
Association request
Association response
AP sends the associated security parameters
Station sets selected security parameters
802.1X controlled port blocked
802.1x EAP request
802.1x EAP response
Access request (EAP request)
Extensible Authentication Protocol Exchange
Accept/EAP-success key material
802.1x EAP success
802.1X controlled port blocked

Figure 18.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

IEEE 802.1X Access Control Approach

- Port-Based Network Access Control
- The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard
- 802.1X uses:
    - Controlled ports
        - Allows the exchange of PDUs between a supplicant and other systems on the LAN only if the current state of the supplicant authorizes such an exchange
    - Uncontrolled ports
        - Allows the exchange of PDUs between the supplicant and the other AS, regardless of the authentication state of the supplicant

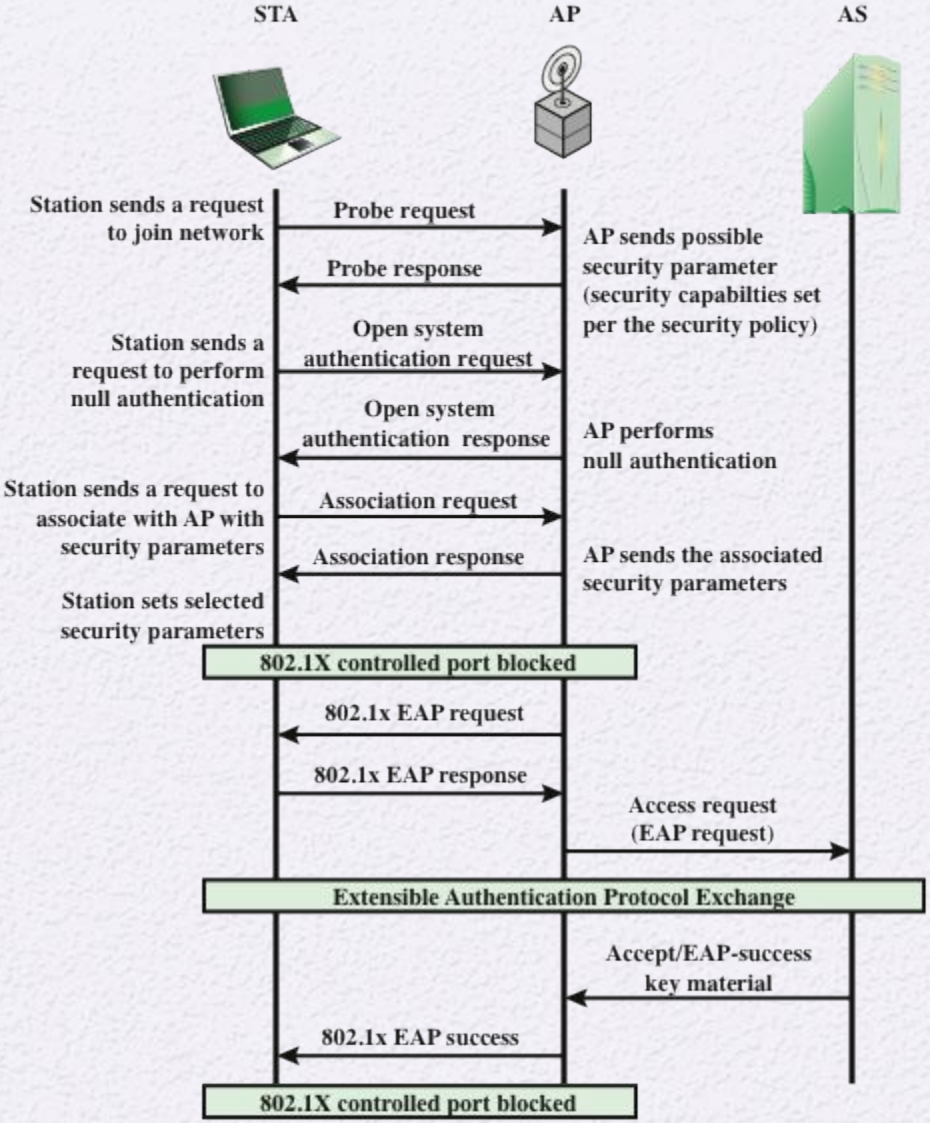
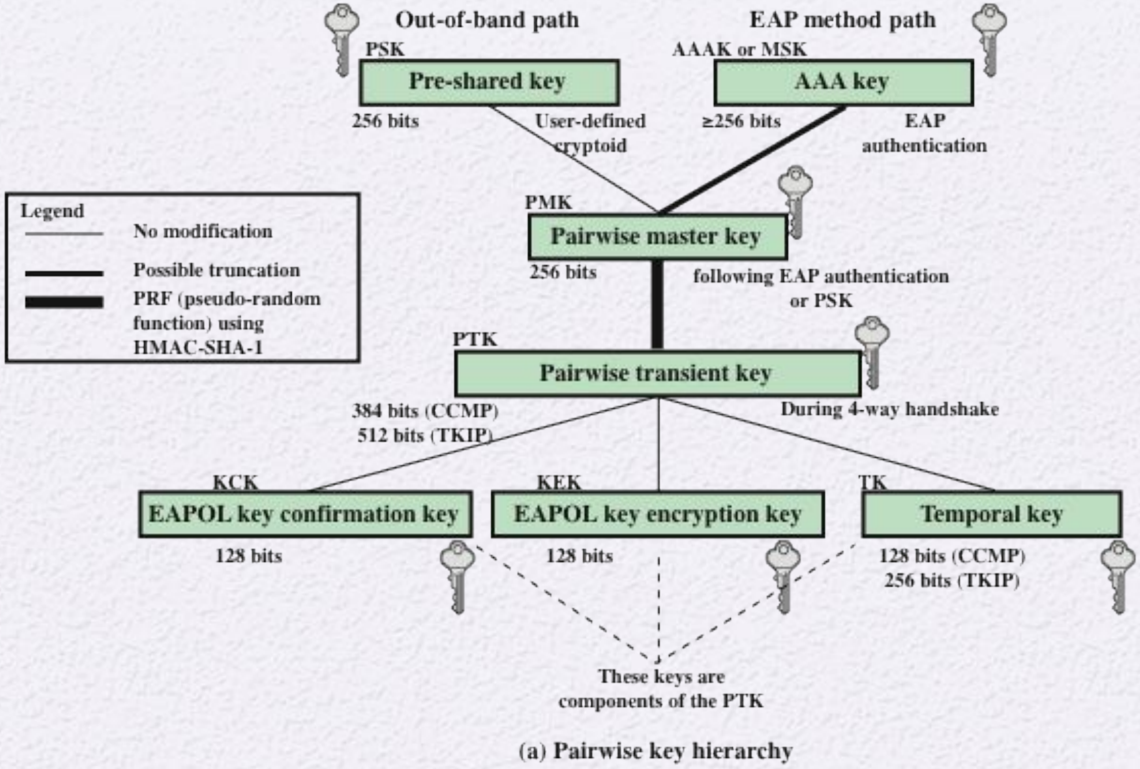

STA
AP
AS
Station sends a request to join network
Probe request
AP sends possible security parameter (security capabilties set per the security policy)
Probe response
Station sends a request to perform null authentication
Open system authentication request
Open system authentication response
AP performs null authentication
Station sends a request to associate with AP with security parameters
Association request
Association response
AP sends the associated security parameters
Station sets selected security parameters
802.1X controlled port blocked
802.1x EAP request
802.1x EAP response
Access request (EAP request)
Extensible Authentication Protocol Exchange
Accept/EAP-success key material
802.1x EAP success
802.1X controlled port blocked

Figure 18.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association



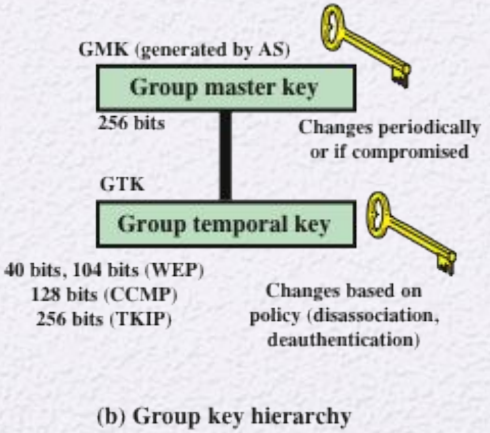
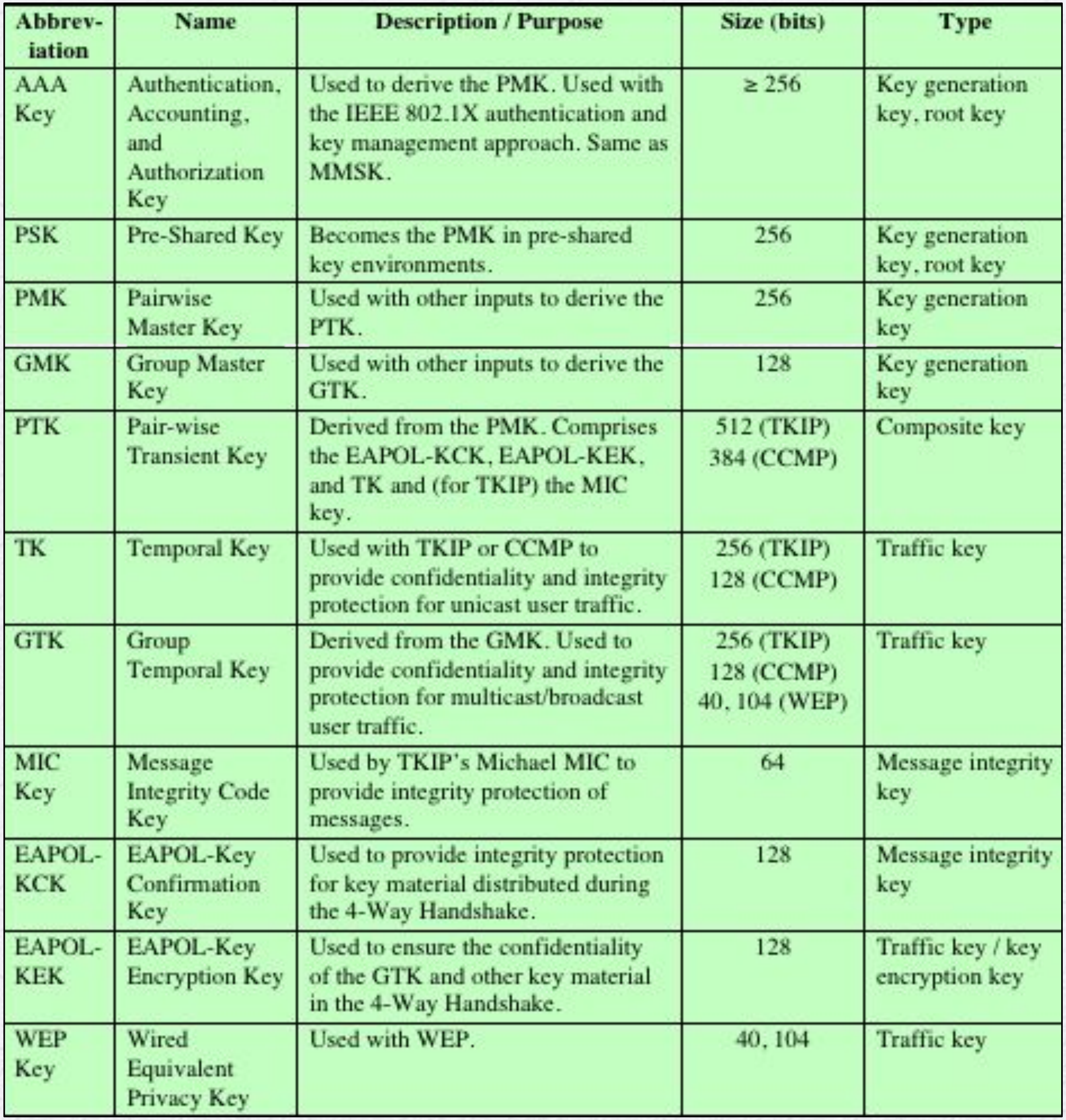


Figure 18.9 IEEE 802.11i Key Hierarchies

Table 18.3

IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols



Abbreviation	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

Pairwise Keys

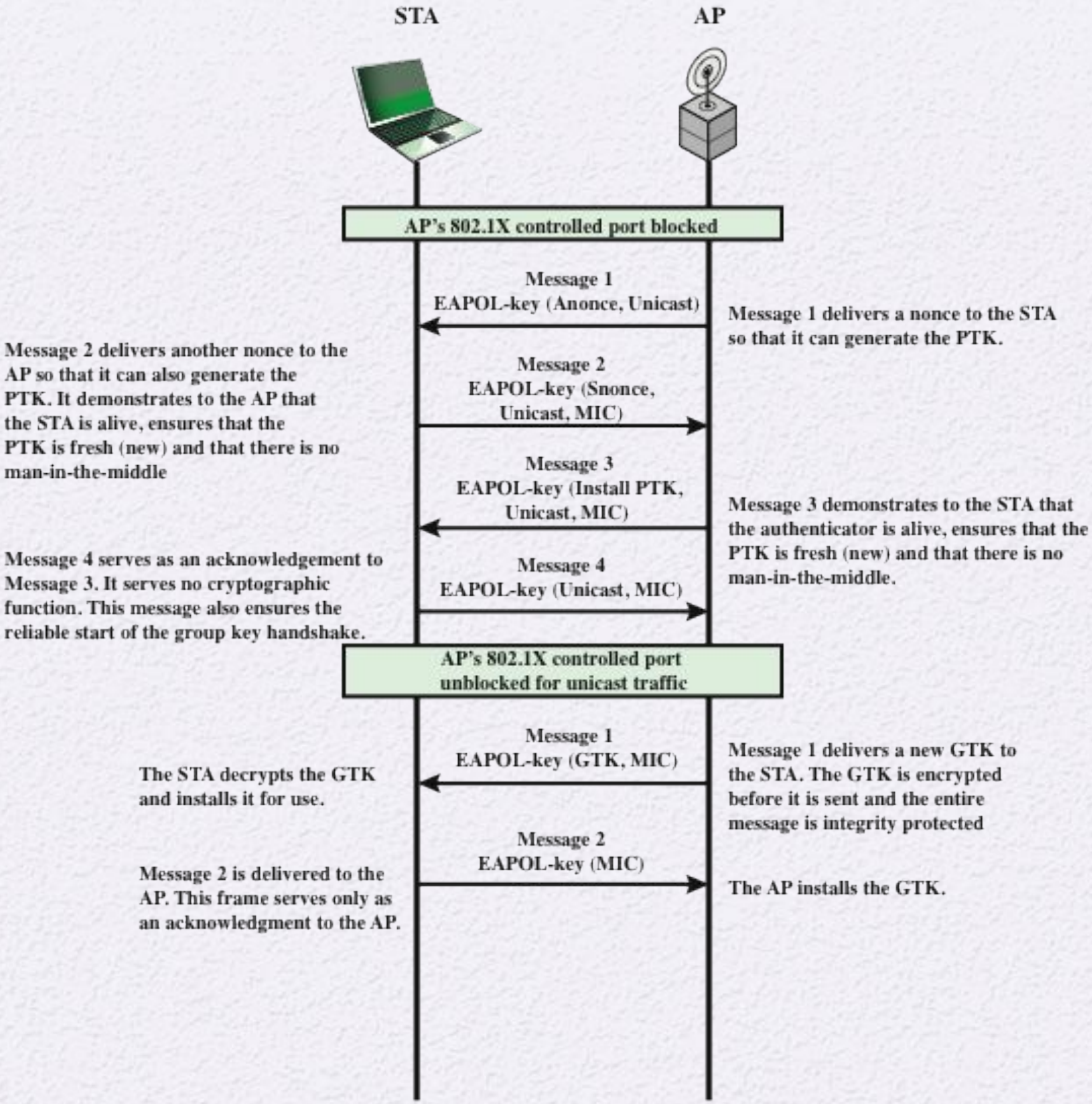
- **Used for communication between a pair of devices, typically between a STA and an AP**
  - These keys form a hierarchy beginning with a master key from which other keys are derived dynamically and used for a limited period of time
- **Pre-shared key (PSK)**
  - A secret key shared by the AP and a 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:

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
    - IEEE 802.11i requires that its value is computationally indistinguishable from random
    - Distributed securely using the pairwise keys that are already established
    - Is changed every time a device leaves the network



STA

AP

AP's 802.1X controlled port blocked

Message 1
EAPOL-key (Anonce, Unicast)

Message 1 delivers a nonce to the STA so that it can generate the PTK.

Message 2 delivers another nonce to the AP so that it can also generate the PTK. It demonstrates to the AP that the STA is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle

Message 2
EAPOL-key (Snonce, Unicast, MIC)

Message 3
EAPOL-key (Install PTK, Unicast, MIC)

Message 3 demonstrates to the STA that the authenticator is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.

Message 4 serves as an acknowledgement to Message 3. It serves no cryptographic function. This message also ensures the reliable start of the group key handshake.

Message 4
EAPOL-key (Unicast, MIC)

AP's 802.1X controlled port unblocked for unicast traffic

Message 1
EAPOL-key (GTK, MIC)

Message 1 delivers a new GTK to the STA. The GTK is encrypted before it is sent and the entire message is integrity protected

The STA decrypts the GTK and installs it for use.

Message 2
EAPOL-key (MIC)

Message 2 is delivered to the AP. This frame serves only as an acknowledgment to the AP.

The AP installs the GTK.

Figure 18.10 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake

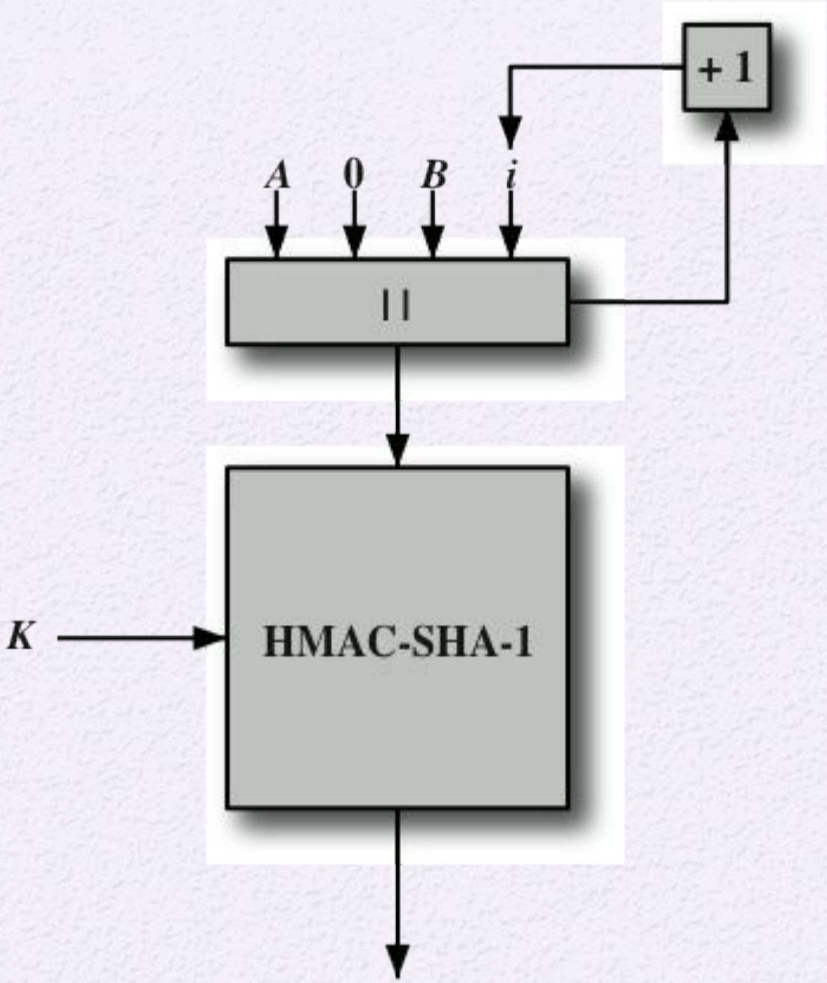
Protected Data Transfer Phase

- IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs:
  - Temporal Key Integrity Protocol (TKIP)
    - Designed to require only software changes to devices that are implemented with WEP
    - Provides two services:
      - Message integrity
      - Data confidentiality
  - Counter Mode-CBC MAC Protocol (CCMP)
    - Intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme
    - Provides two services:
      - Message integrity
      - Data confidentiality

IEEE 802.11i Pseudorandom Function (PRF)

- Used at a number of places in the IEEE 802.11i scheme (to generate nonces, to expand pairwise keys, to generate the GTK)
    - Best security practice dictates that different pseudorandom number streams be used for these different purposes

- Built on the use of HMAC-SHA-1 to generate a pseudorandom bit stream



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

Figure 18.11 IEEE 802.11i Pseudorandom Function

Summary

- Wireless network security
  - Network threats
  - Security measures
- Mobile device security
  - Security threats
  - Security strategy
- IEEE 802.11 wireless LAN overview
  - Wi-Fi Alliance
  - IEEE 802 protocol architecture
  - IEEE 802.11 network components and architectural model
  - IEEE 802.11 services

- IEEE 802.11i wireless LAN security
  - IEEE 802.11i services
  - IEEE 802.11i phases of operation
  - Discovery phase
  - Authentication phase
  - Key management phase
  - Protected data transfer phase
  - The IEEE 802.11i pseudorandom function