Chapter 18

WIRELESS NETWORK SECURITY

Wireless Security

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

Channel

Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks

Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

Mobility

Wireless devices are far more portable and mobile than wired devices

This mobility results in a number of risks

Resources

Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

Accessibility

Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations

This greatly increases their vulnerability to physical attacks

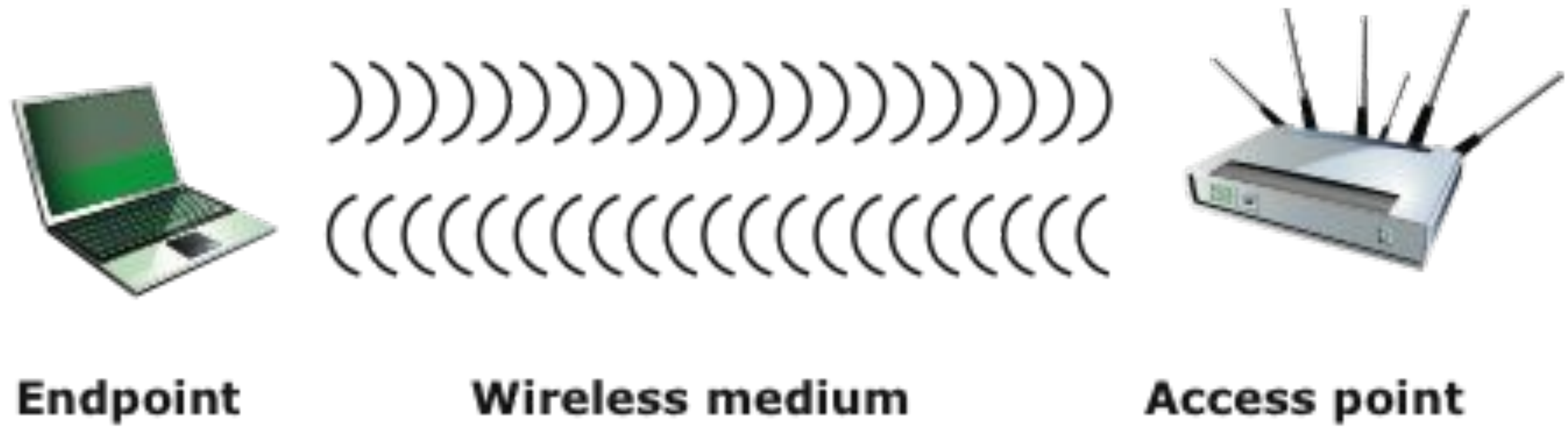


Figure 18.1 Wireless Networking Components

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

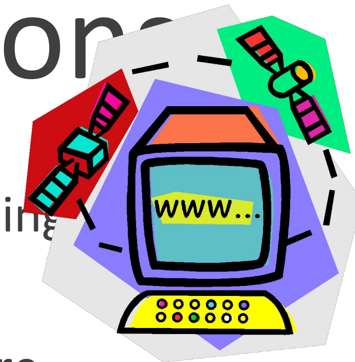
Denial of service (DoS)

- 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

- Use encryption
- Use antivirus, antispyware software and a firewall
- Turn off identifier broadcasting
- Change the identifier on your router from the default
- Change your router's pre-set password for administration
- Allow only specific computers to access your wireless network

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:

Lack of physical security controls

- The security policy for mobile devices must be based on the assumption that any mobile device may be stolen or at least accessed by a malicious party

Use of untrusted mobile devices

- The organization must assume that not all devices are trustworthy

Use of untrusted networks

- The security policy must be based on the assumption that the networks between the mobile device and the organization are not trustworthy

Use of untrusted content

- Mobile devices may access and use content that other computing devices do not encounter

Use of applications created by unknown parties

- It is easy to find and install third-party applications on mobile devices and this poses the risk of installing malicious software

Interaction with other systems

- Unless an organization has control of all the devices involved in synchronization, there is considerable risk of the organization's data being stored in an unsecured location, plus the risk of the introduction of malware

Use of location services

- An attacker can use location information to determine where the device and user are located, which may be of use to the attacker

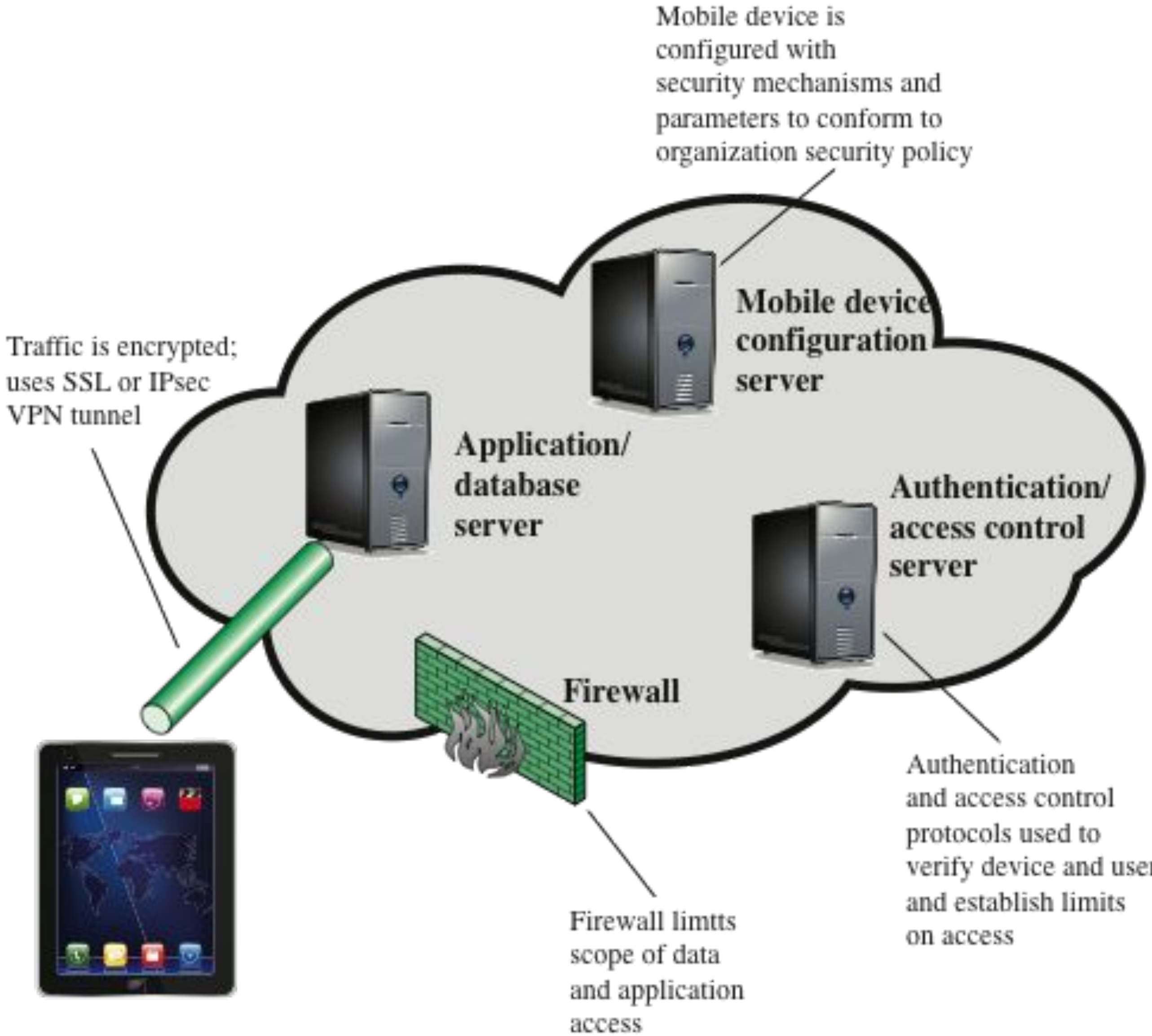


Figure 18.2 Mobile Device Security Elements

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.

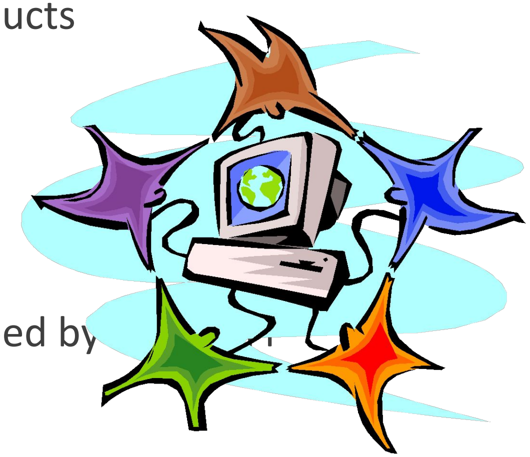
(Table can be found on page 572 in textbook)

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
  Alliance

- Recently the Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards
  - Referred to as Wi-Fi Protected Access (WPA)

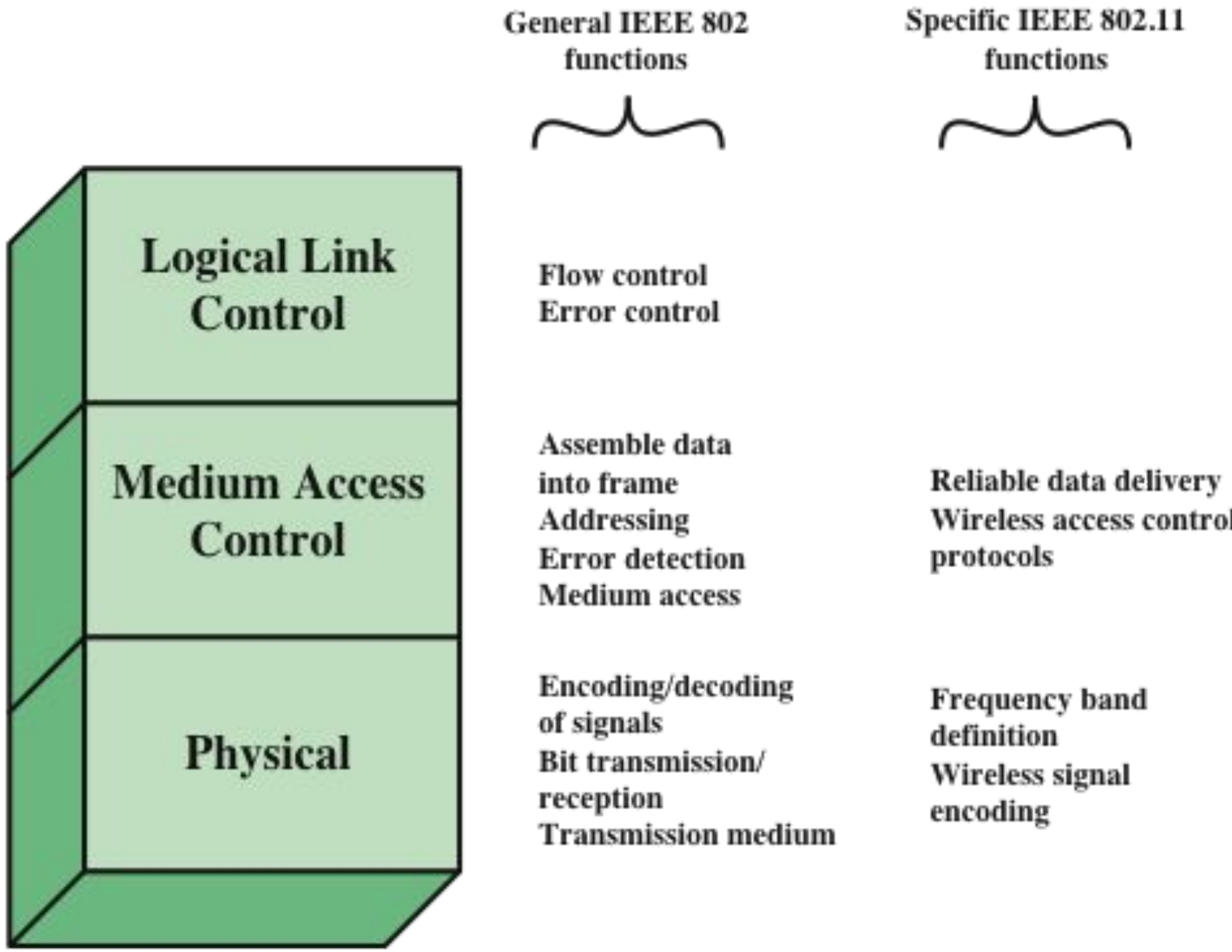


Figure 18.3 IEEE 802.11 Protocol Stack

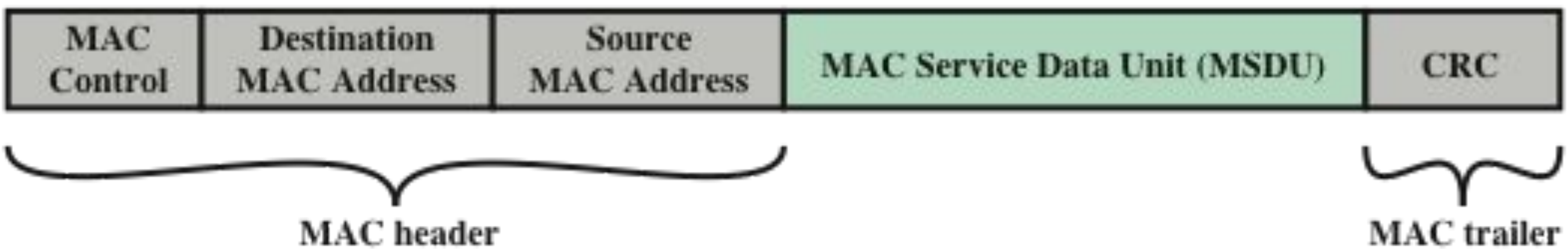


Figure 18.4 General IEEE 802 MPDU Format

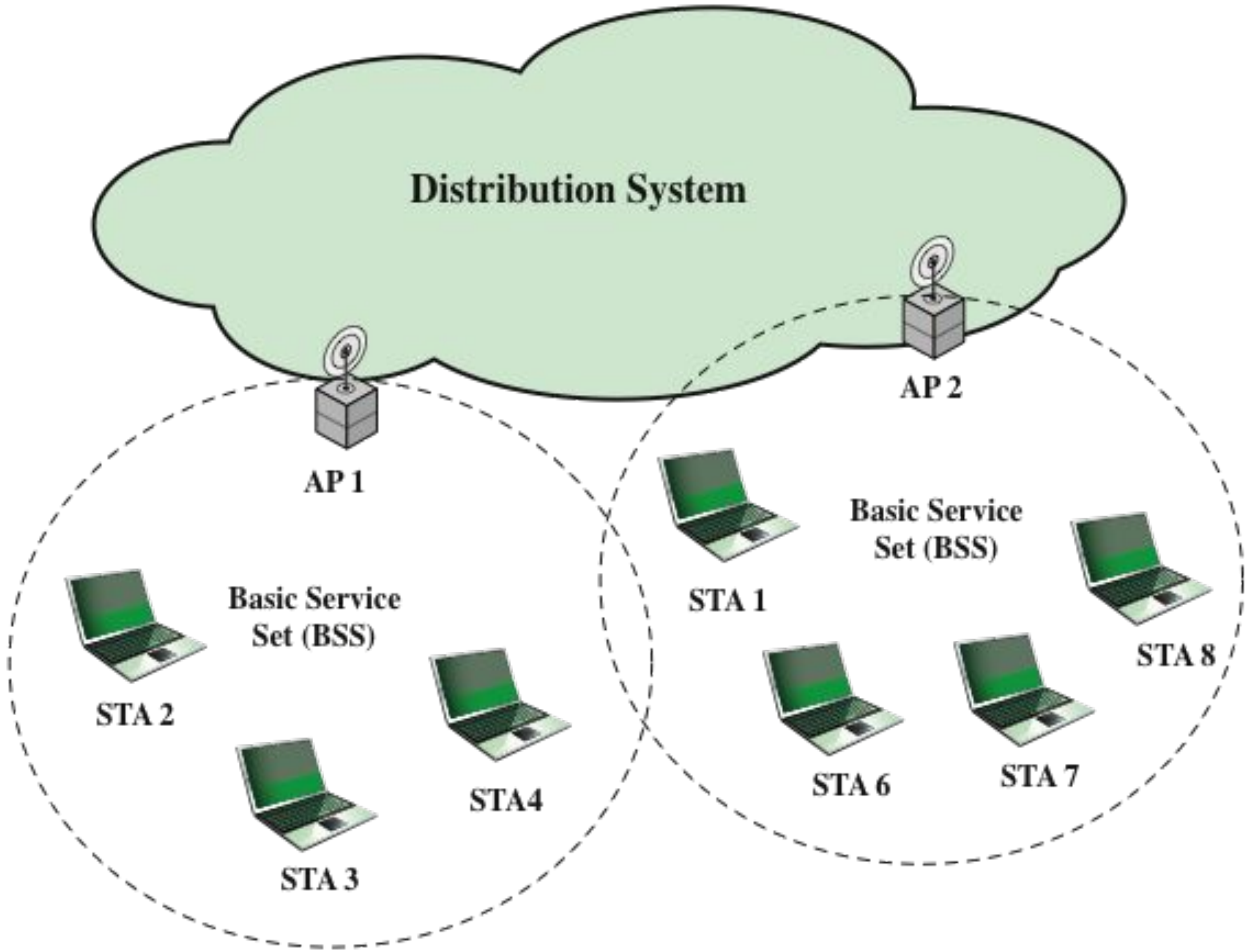


Figure 18.5 IEEE 802.11 Extended Service Set

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:

Integration

- Enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN
- Takes care of any address translation and media conversion logic required for the exchange of data

Distribution

- The primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS

Association-Related Services

Transition types based on mobility:

No transition

- A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS

BSS transition

- This is defined as a station movement from one BSS to another BSS within the same ESS
- In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station

ESS transition

- This is defined as a station movement from a BSS in one ESS to a BSS within another ESS
- Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed
- Disruption of service is likely to occur

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

Wired Equivalent Privacy (WEP)

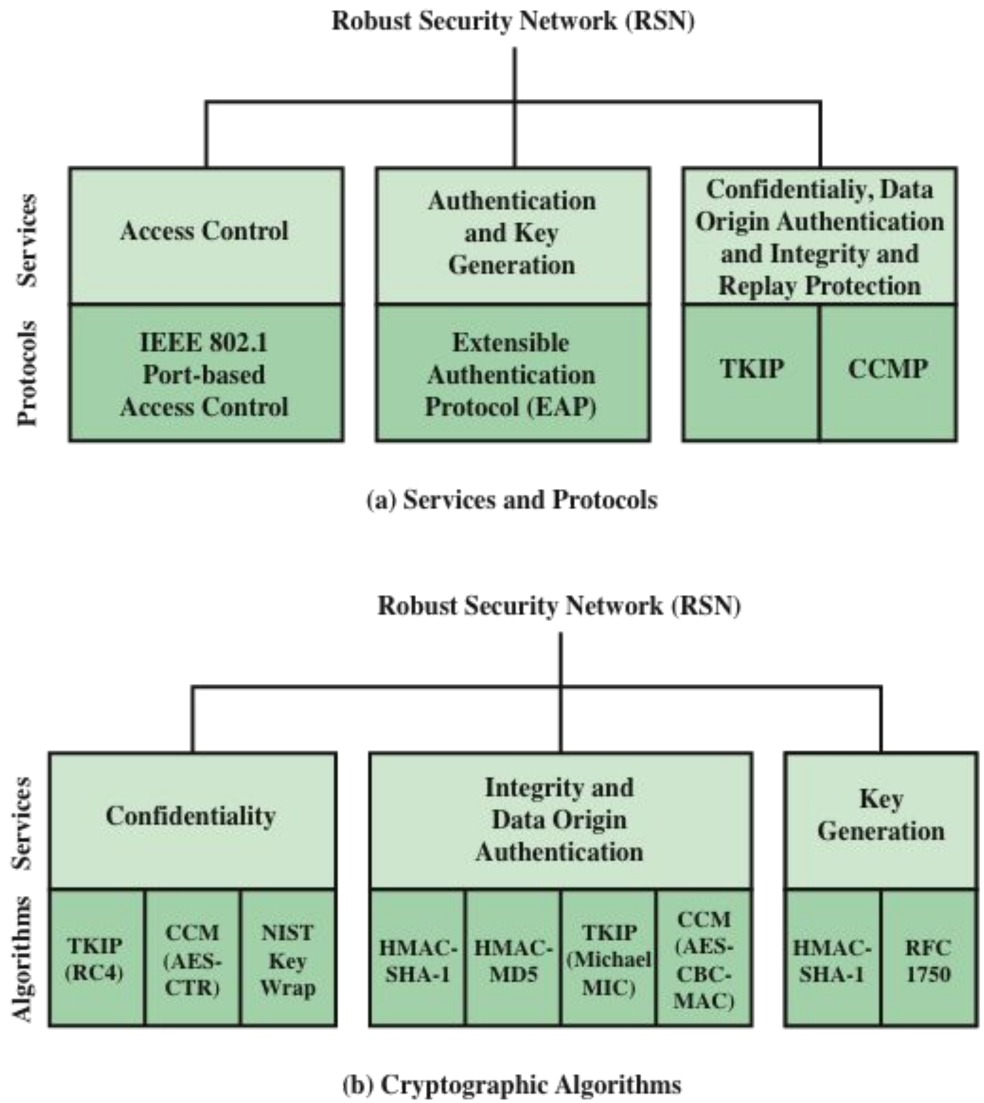
- The privacy portion of the 802.11 standard
- Contained major weaknesses

Wi-Fi Protected Access (WPA)

- A set of security mechanisms that eliminates most 802.11 security issues
- Based on the current state of the 802.11i standard

Robust Security Network (RSN)

- Final form of the 802.11i standard
- Complex



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

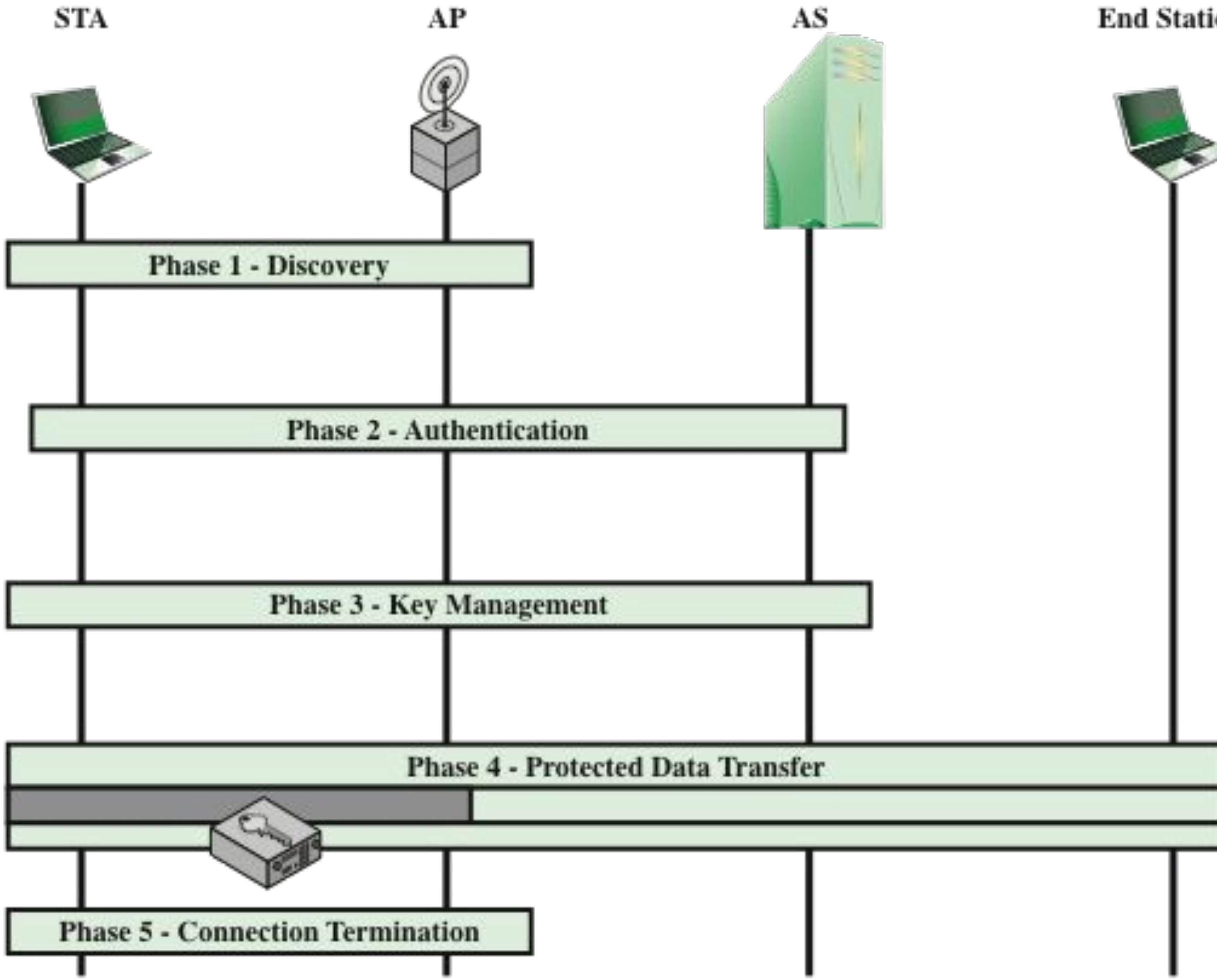


Figure 18.7 IEEE 802.11i Phases of Operation

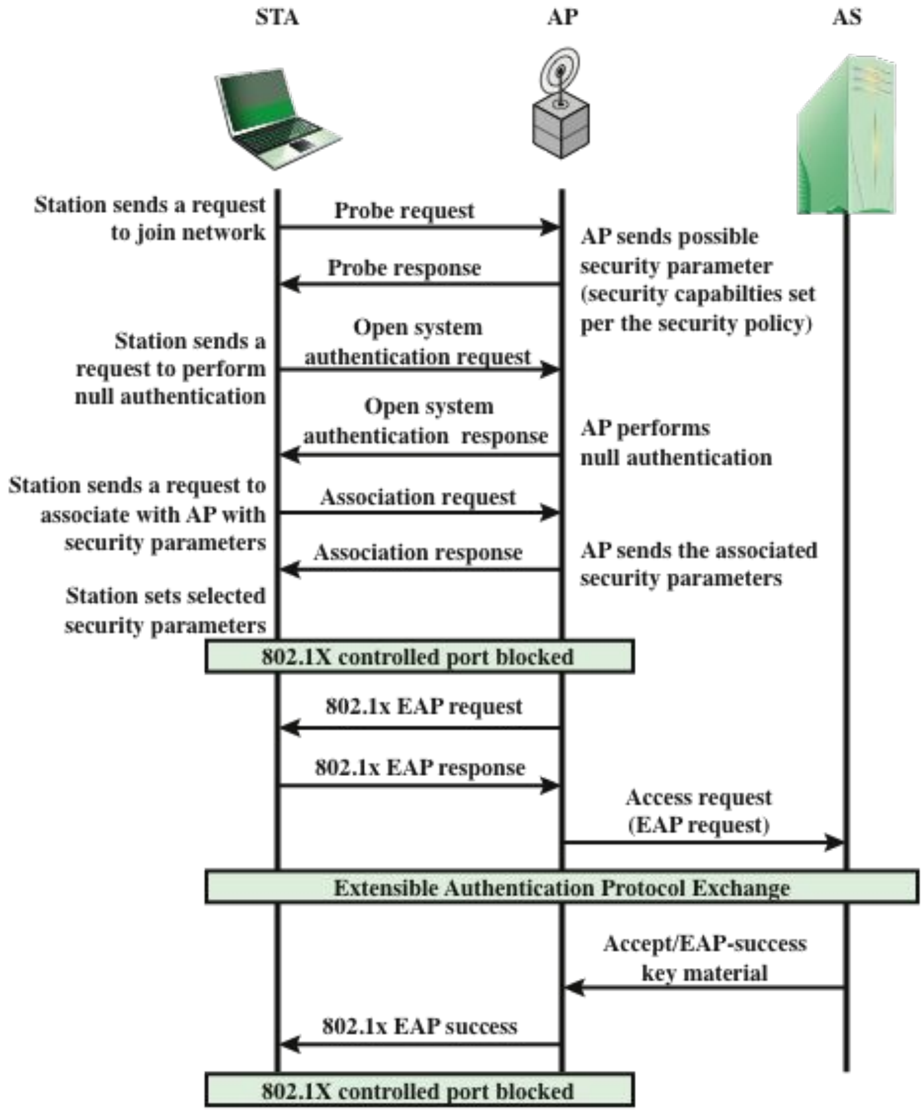


Figure 18.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

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

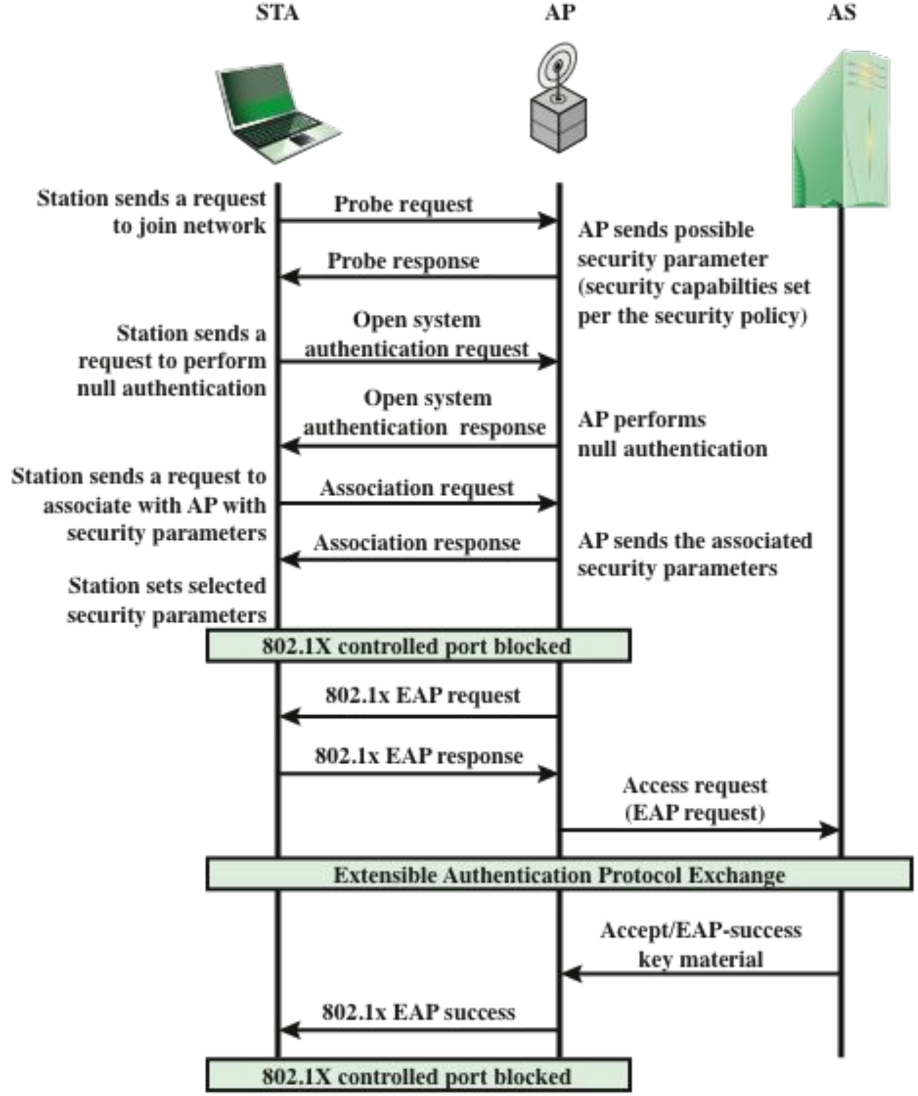


Figure 18.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

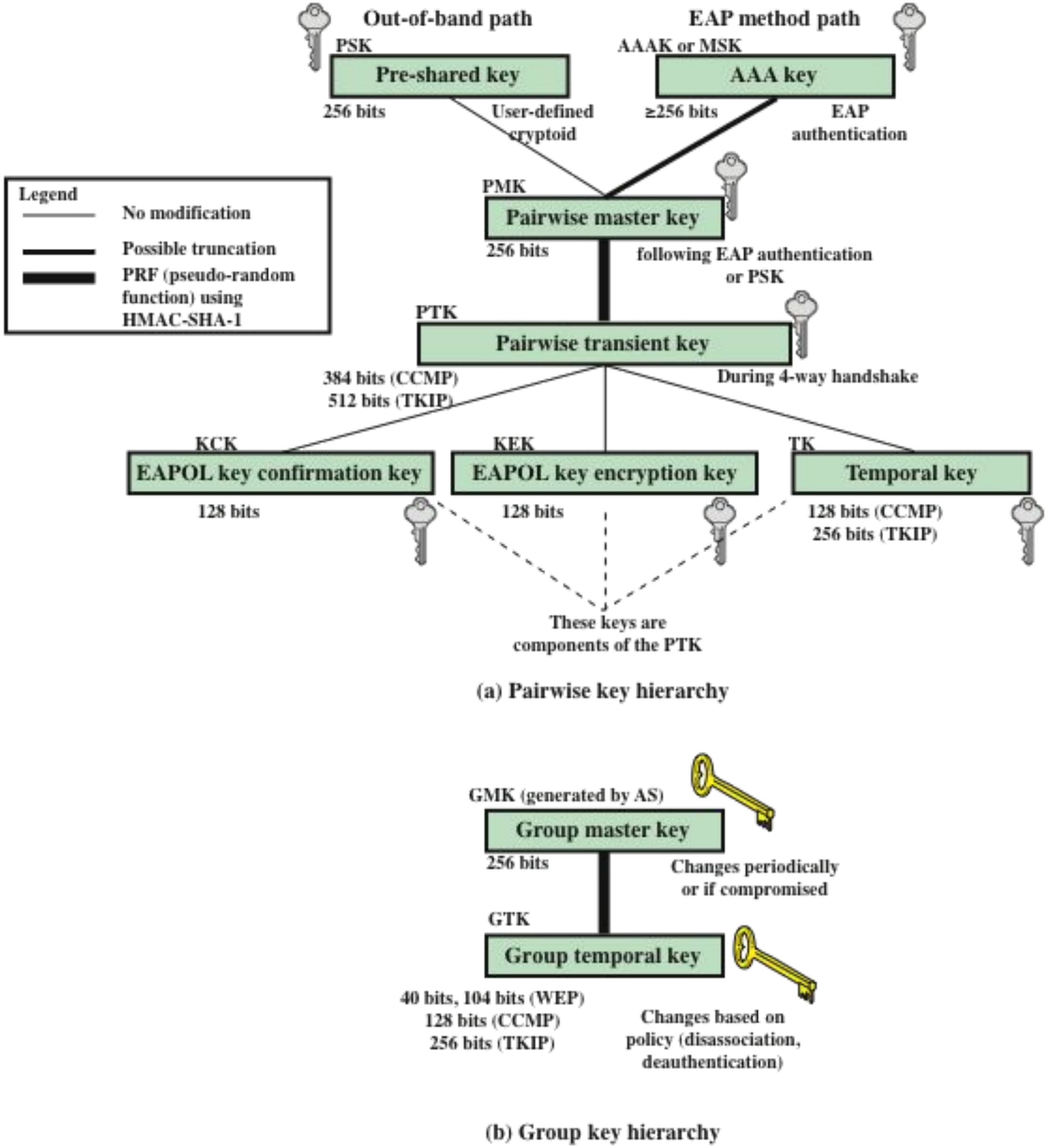


Figure 18.9 IEEE 802.11i Key Hierarchies

Table 18.3

IEEE 802.11i Keys for Data Confidentiality and Integrity Protocols

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

(Table can be found on page 586 in the textbook)

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
- An entity that possesses the PMK is authorized to use the link

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
  - 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

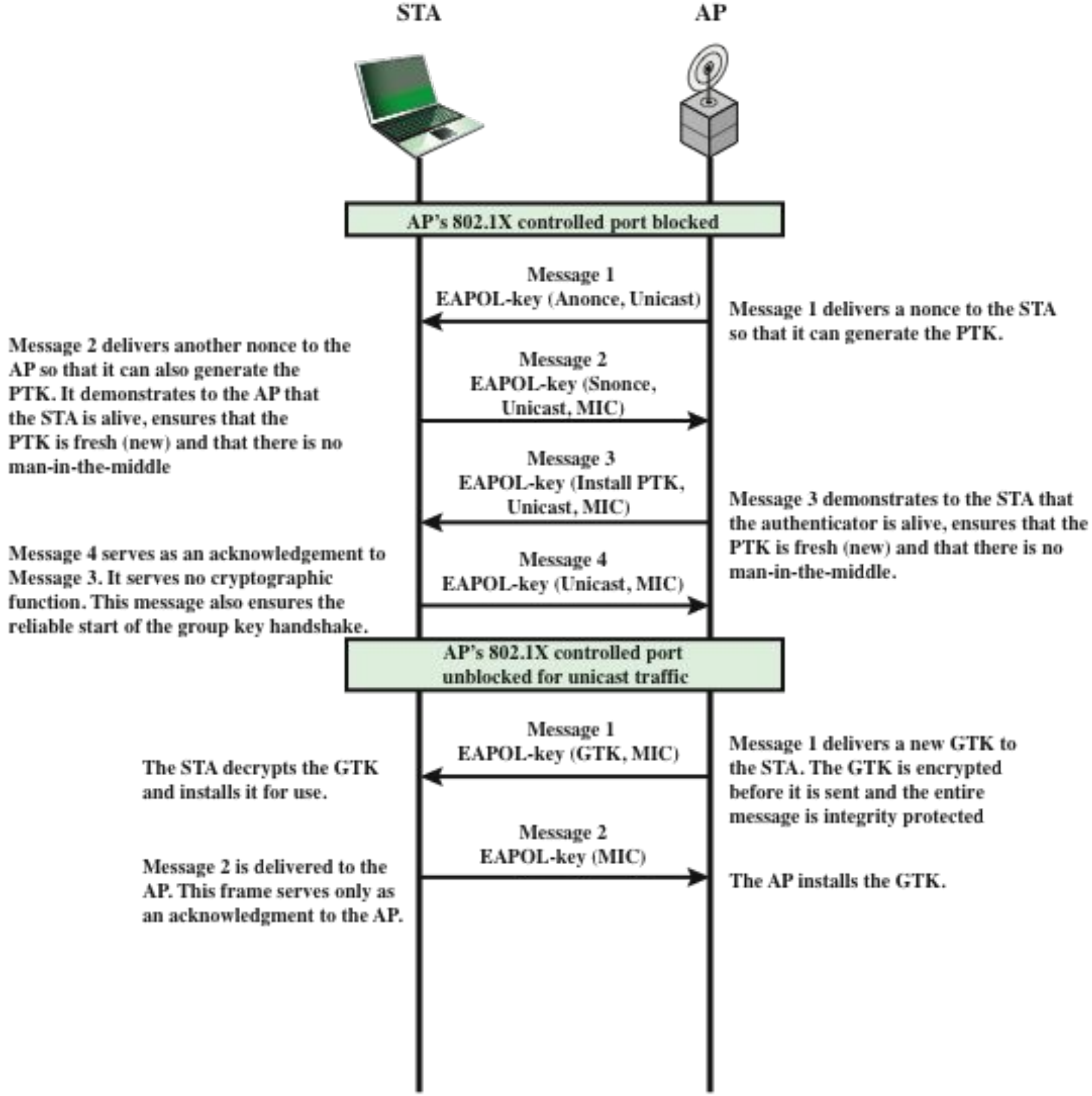


Figure 18.10 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake

Protected Data Transfer Phase

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

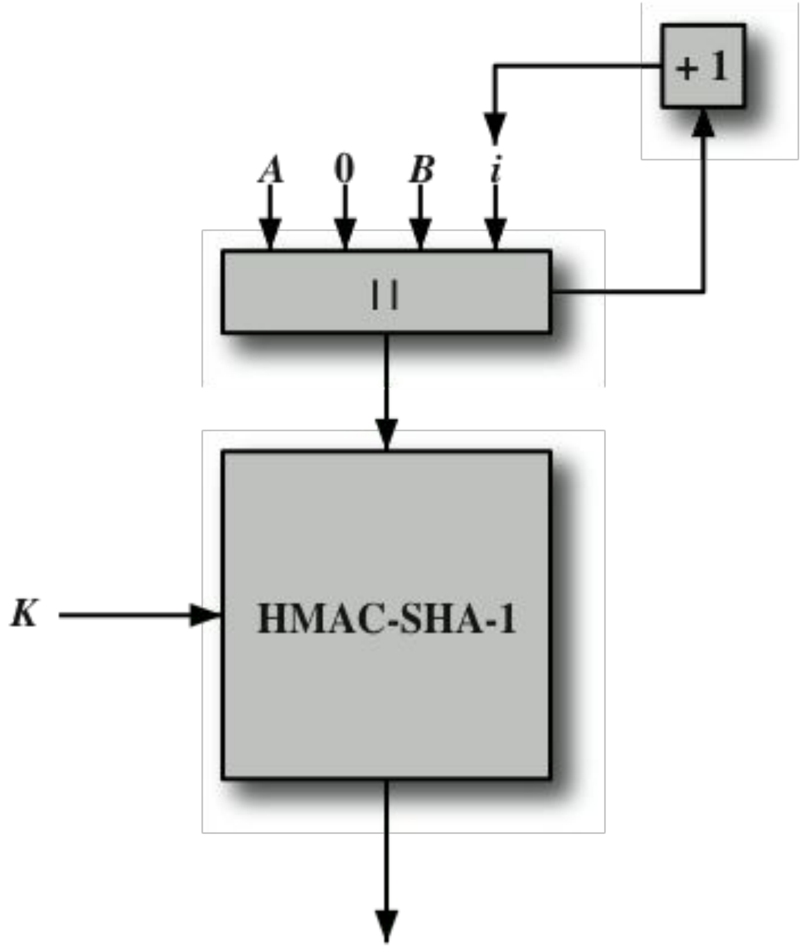
- Temporal Key Integrity Protocol (TKIP)
  - Designed to require only software changes to devices that are implemented with WEP
  - Provides two services:
    - Message integrity
    - Data confidentiality
- Counter Mode-CBC MAC Protocol (CCMP)
  - Intended for newer IEEE 802.11 devices that are equipped 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 = HMAC-SHA-1(K, $A \| 0 \| B \| i$)

Figure 18.11 IEEE 802.11i Pseudorandom Function

Summary

Wireless network security

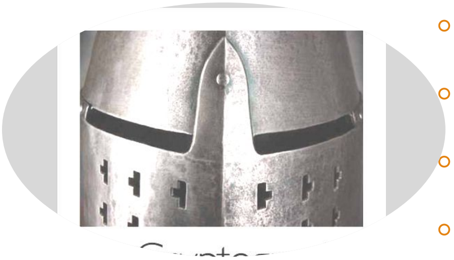
- Network threats
- Security measures

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