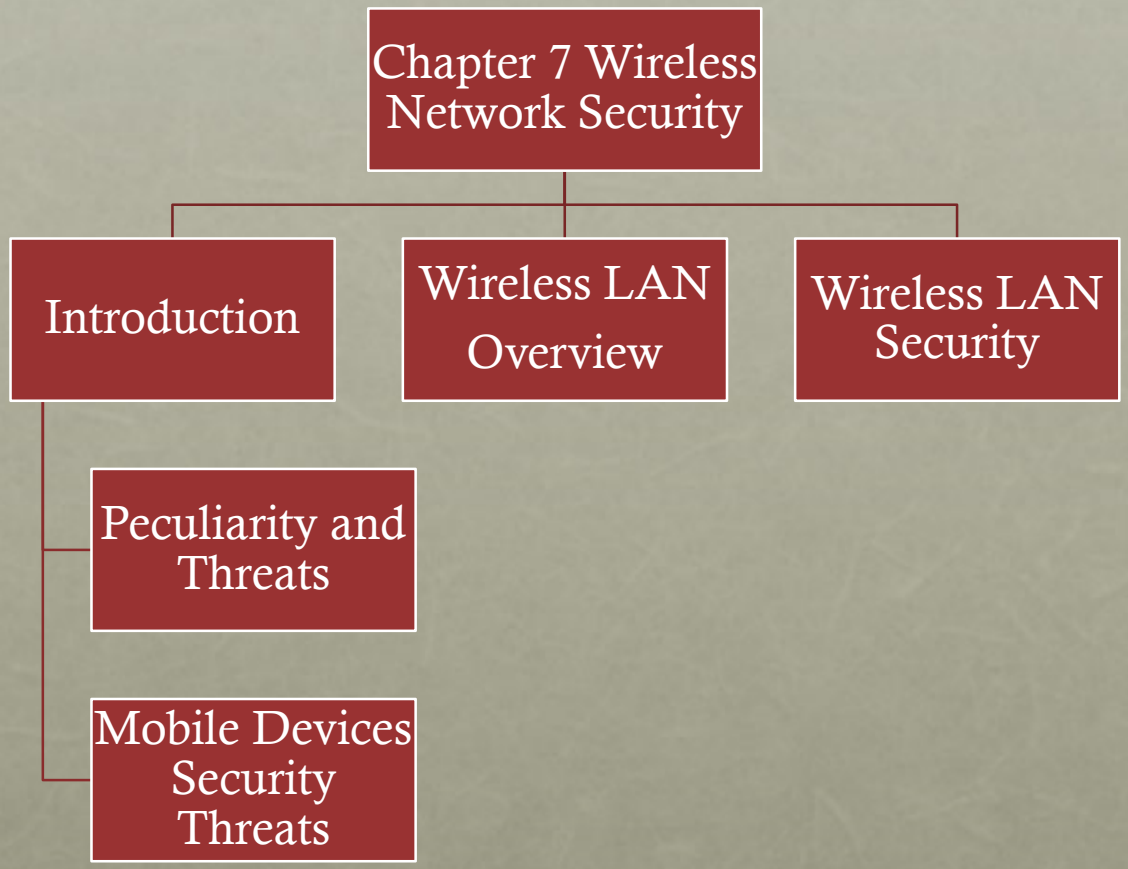
CHAPTER 7

Wireless Network Security

OUTLINE


Chapter 7 Wireless Network Security
Introduction
Wireless LAN Overview
Wireless LAN Security
Peculiarity and Threats
Mobile Devices Security Threats

PECULIARITY OF WIRELESS NETWORKS

- 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

WIRELESS NETWORKING COMPONENTS

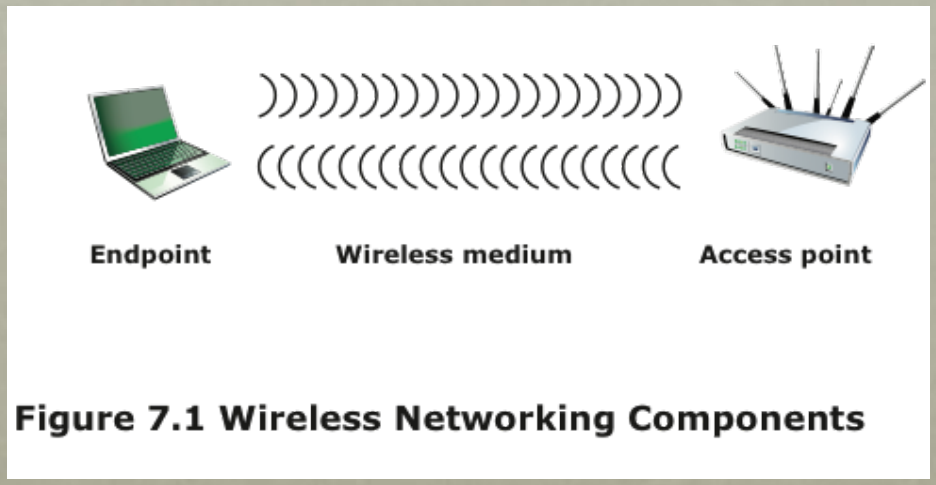


Figure 7.1 Wireless Networking Components

- **The wireless client** can be: a cell phone, a Wi-Fi–enabled laptop or tablet, a wireless sensor, a Bluetooth device, and so on.
- **The wireless access point** provides a connection to the network or service. Examples of access points are cell towers, Wi-Fi hotspots, and wireless access points to wired local or wide area networks.
- **The transmission medium**, which carries the radio waves for data transfer, is also a source of vulnerability.

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

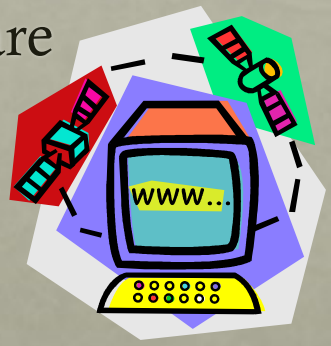
THE EAVESDROPPER

Nicolaes Maes 1600’s

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 and authentication** are effective against eavesdropping and/or active attacks.
  - **DoS (details later) can also be countered** through site surveys to identify other wireless devices using the same frequency.



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

RECOMMENDATIONS FOR 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

The central element in all of these changes is the mobile computing device.

MOBILE DEVICES SECURITY THREATS

- Major security concerns for mobile devices (SP 800-14 Guidelines)

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 (e.g. QR Code)

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

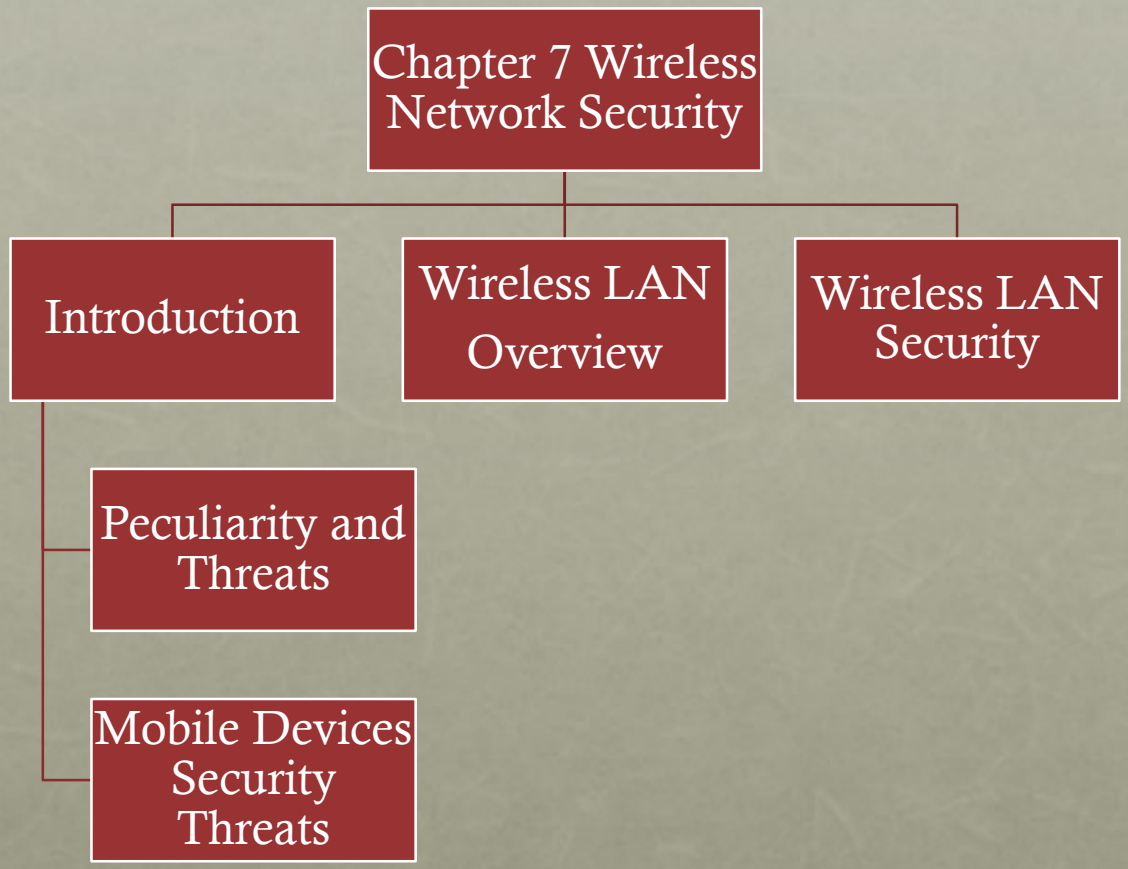
Interaction with other systems

- 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

OUTLINE


Chapter 7 Wireless Network Security
Introduction
Wireless LAN Overview
Wireless LAN Security
Peculiarity and Threats
Mobile Devices Security Threats

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

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)

IEEE 802 vs IEEE 802.11 Functions

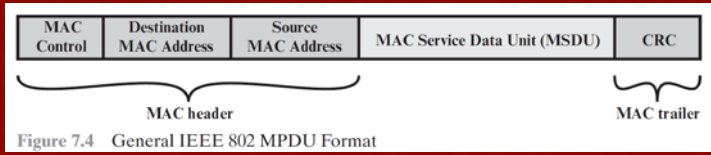


Figure 7.4 General IEEE 802 MPDU Format

MPDU Comprises:

- MAC Control
- Destination MAC
- Source MAC
- MAC Service Data Unit (MSDU): Data from higher layer
- CRC: cyclic redundancy check, which is used for error detection

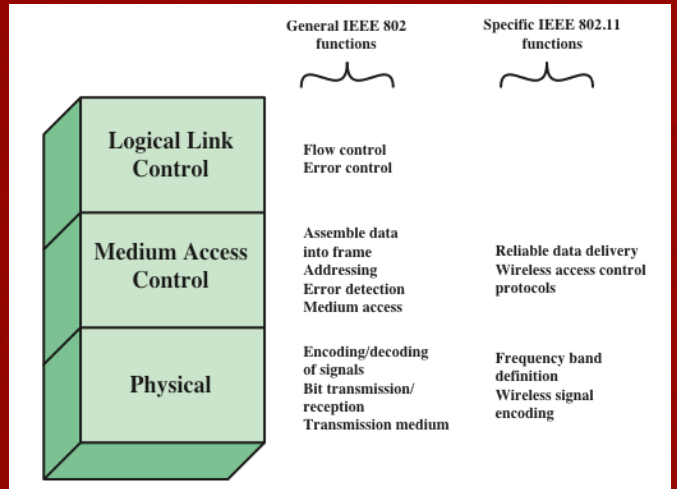


Figure 7.3 IEEE 802.11 Protocol Stack

What is unique in IEEE 802.11

- Physical layer
  - Which frequency bands should be used
  - Unique encoding schemes that are more suitable for wireless transmission
- MAC
  - For example, we will need to use CSMA-CA instead of CSMA-CD
- Logical Link Control
  - LLC is agnostic to MAC and PHY layer techniques. Hence, no uniqueness for IEEE 802.11.

IEEE 802.11 Network Component and Architecture Model

- The smallest building block of a wireless LAN is a basic service set (**BSS**),
- BSS consists of wireless stations (**STA**) 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**) .

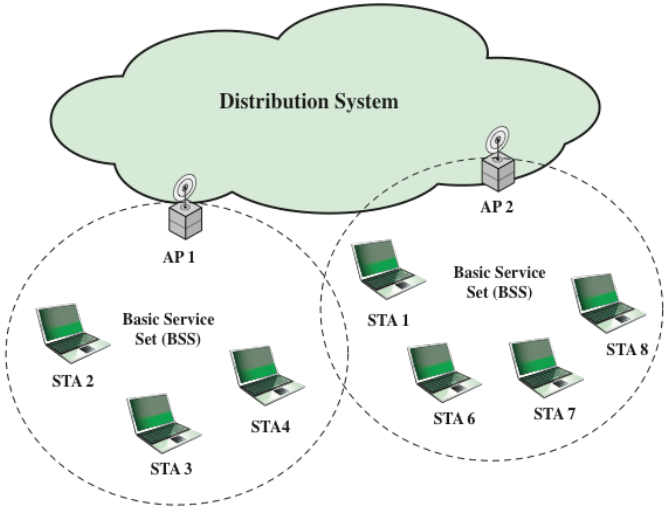


Figure 7.5 IEEE 802.11 Extended Service Set

- The AP functions as a bridge and a relay point.
- In a BSS, client stations do not communicate directly with one another.
- Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame is first sent from the originating station to the AP and then from the AP to the destination station.
- An extended service set (**ESS**) consists of two or more BSS interconnected by a DS.

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.

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

- IEEE 802.11 defines **nine** services that need to be provided by the wireless LAN to achieve functionality equivalent to that which is inherent to wired LANs.

- **Three** of the services are used to control IEEE 802.11 LAN access and confidentiality: authentication, deauthentication and privacy.

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

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

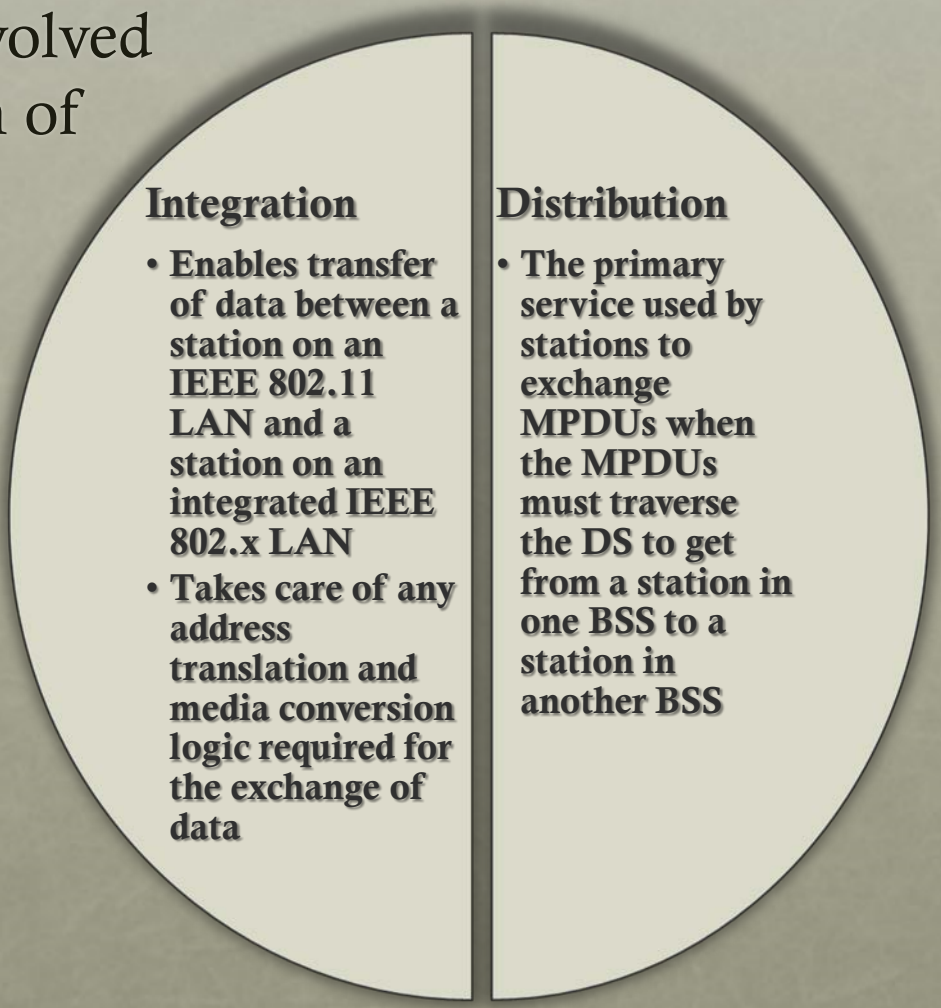
- This is defined as a station movement from one BSS to another BSS within the same ESS
- In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station

ESS transition

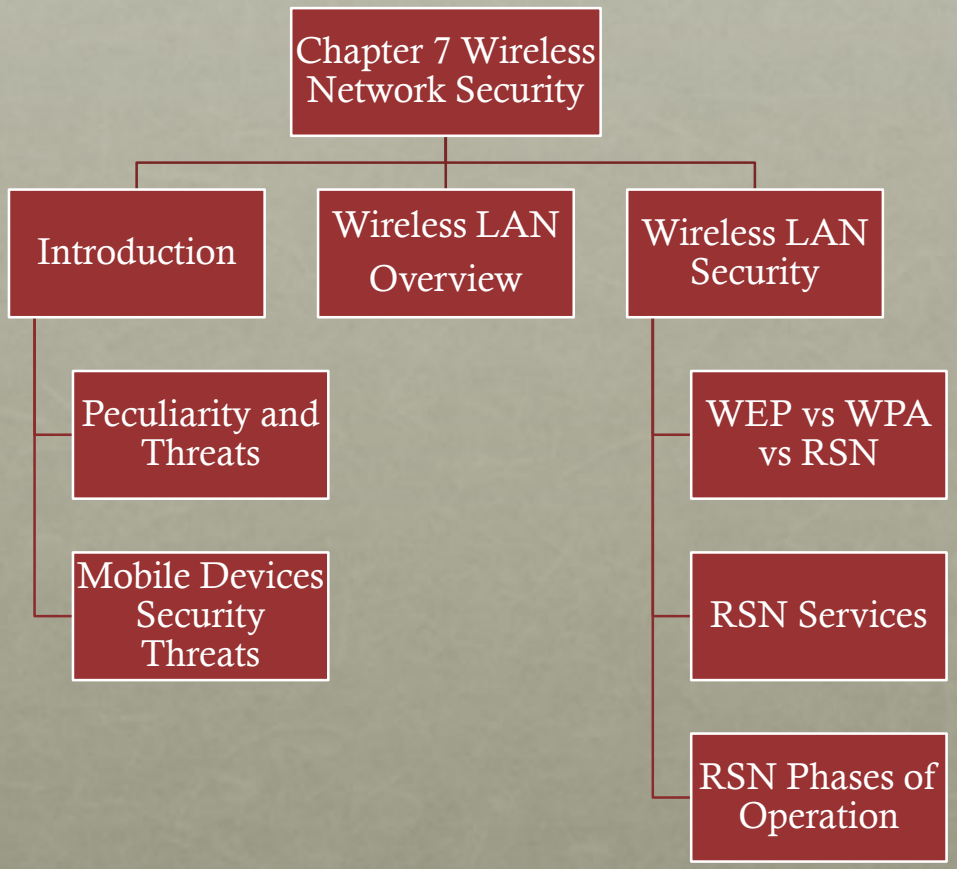
- This is defined as a station movement from a BSS in one ESS to a BSS within another ESS
- Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed
- Disruption of service is likely to occur

DISTRIBUTION OF MESSAGES WITHIN A DS

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

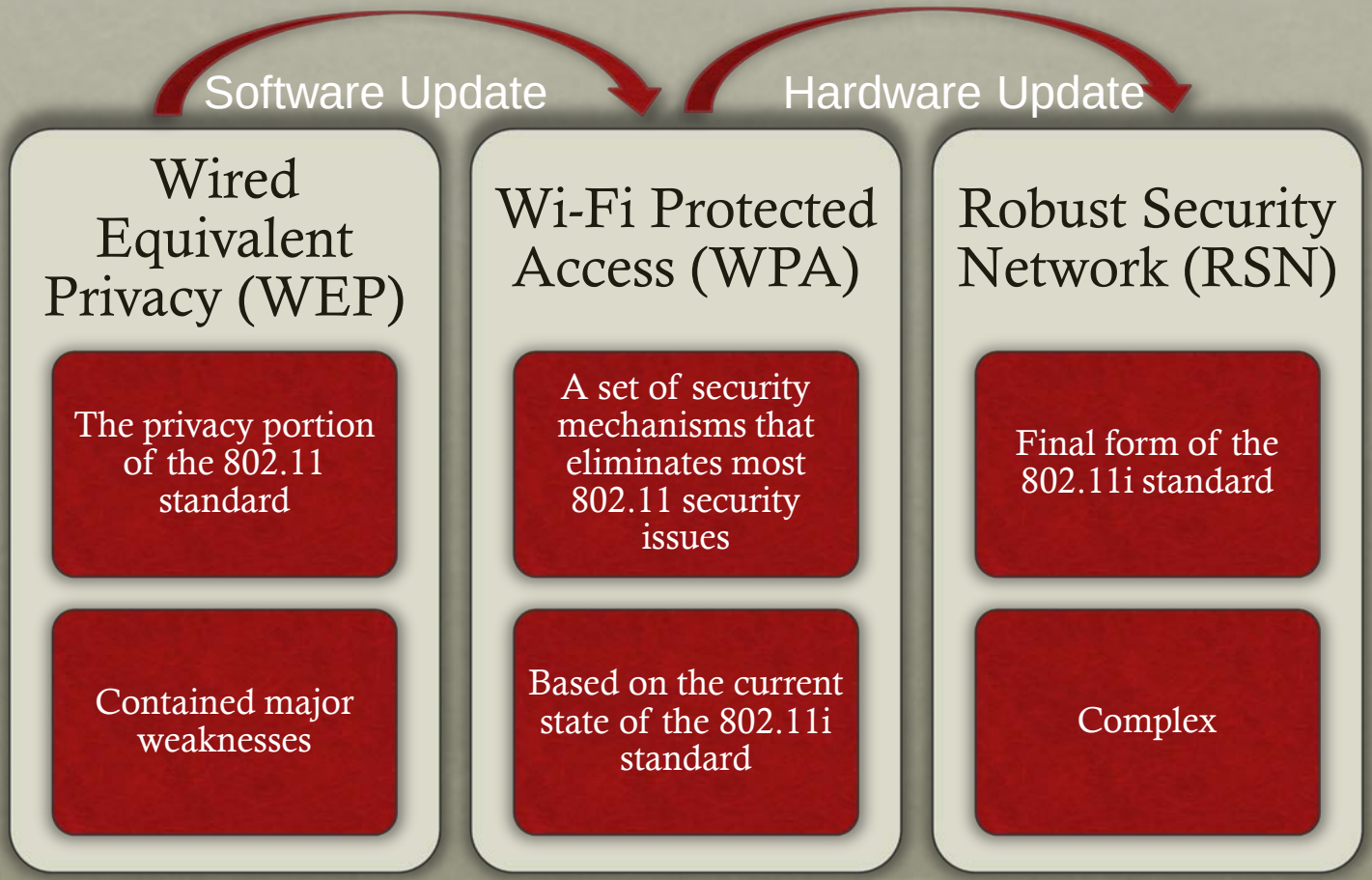


OUTLINE


Chapter 7 Wireless Network Security
Introduction
Wireless LAN Overview
Wireless LAN Security
Peculiarity and Threats
Mobile Devices Security Threats
WEP vs WPA vs RSN
RSN Services
RSN Phases of Operation

IEEE 802.11I WIRELESS LAN SECURITY

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

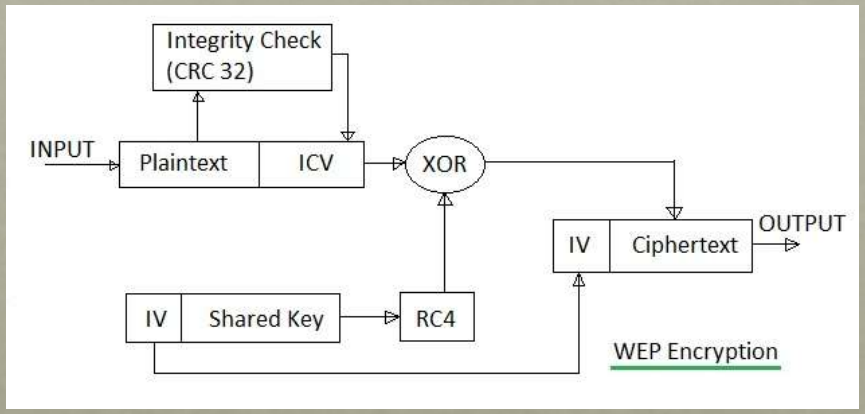


WEP VS WPA VS RSN

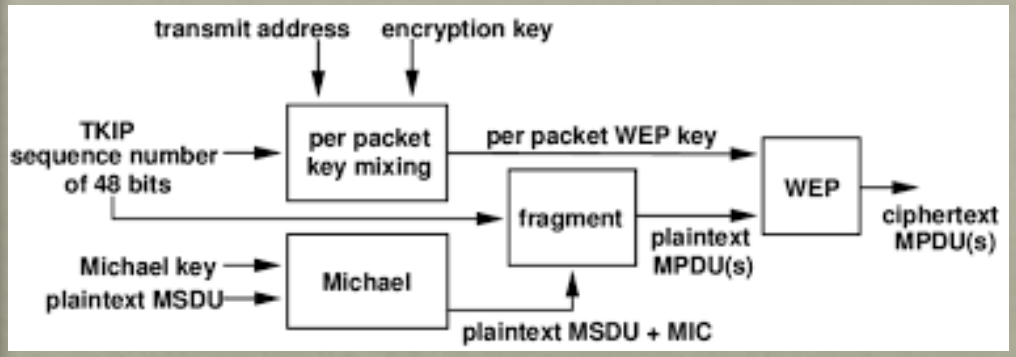
WEP	WPA	RSN (WPA2)
• WEP uses static key • All STAs use same key • Key is extracted directly from the password • You can get the password from network admins	• Uses TKIP • TKIP combines the secret key with an IV that is unique to each STA • New key is generated for new data	Replaces WEP and TKIP
Uses RC4	Uses RC4	AES with CCMP
Key size: 64 and 128 bits	Key size is 256 bits	128 or 256
Data Integrity: CRC-32	Message Authentication Code	CBC - MAC
Replay Attack: No protection	Implements sequence numbers	Implements 48 bits packet number

WEP VS. TKIP VS. CCM

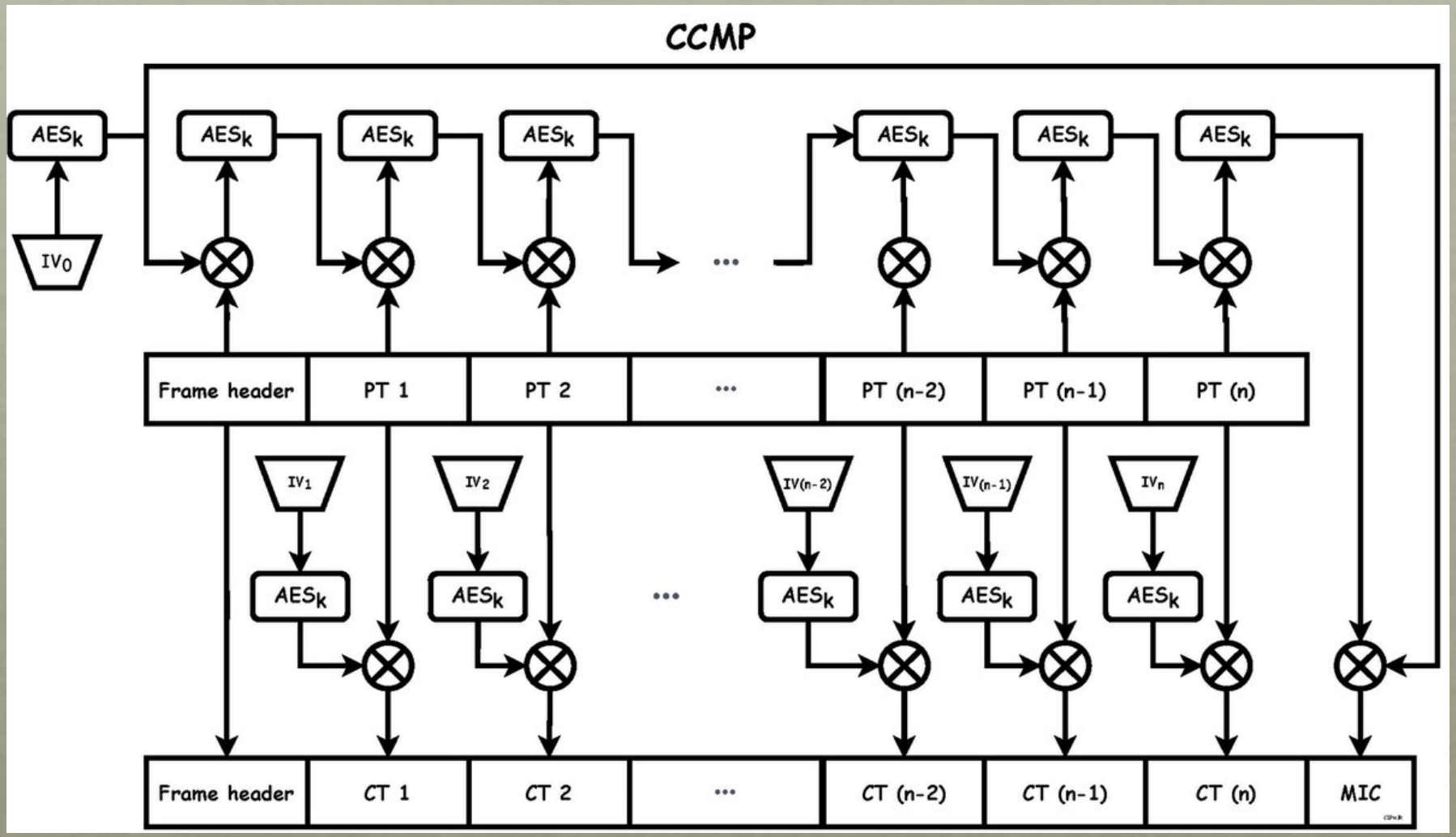
WEP



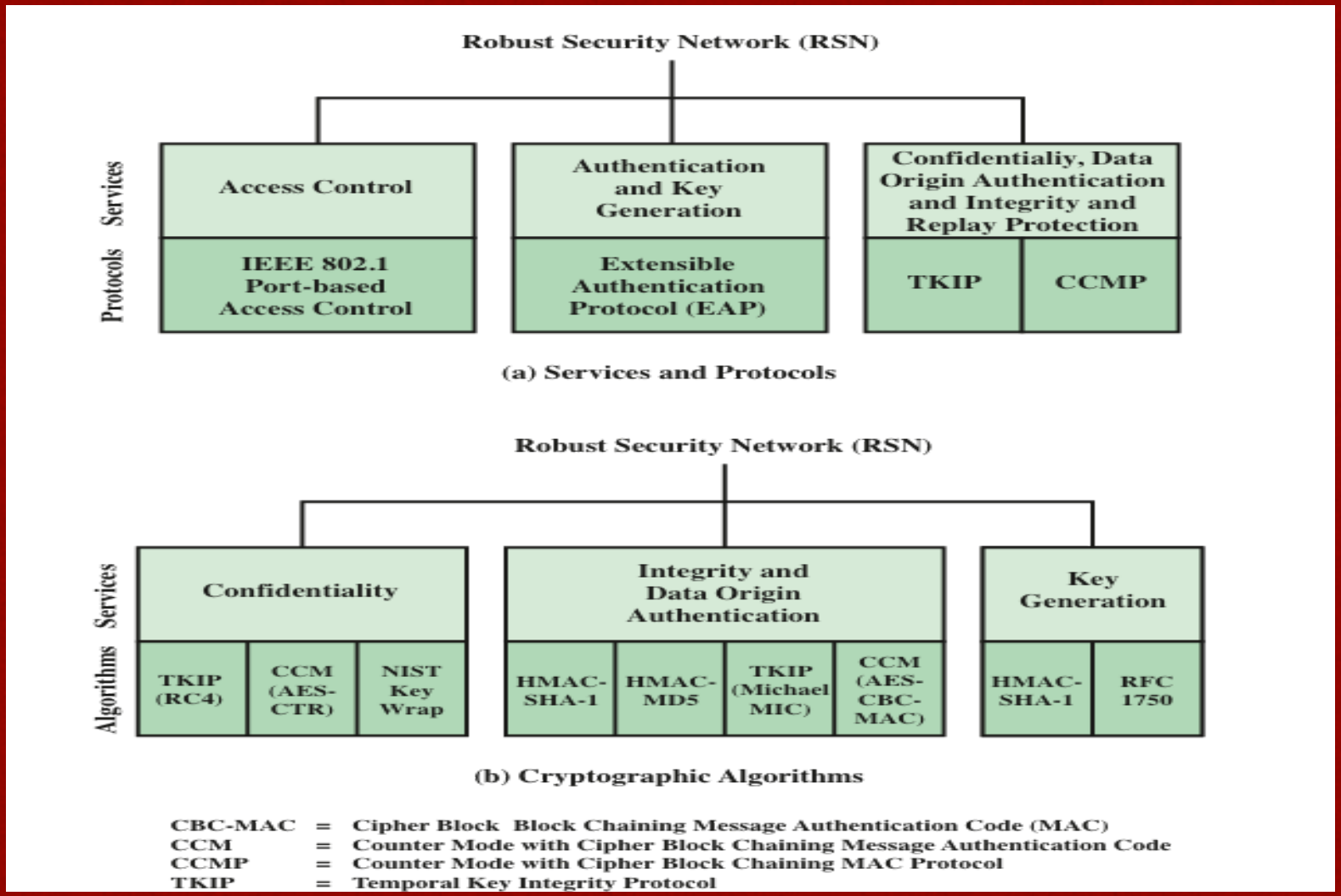
WPA



WEP VS. TKIP VS. CCMP

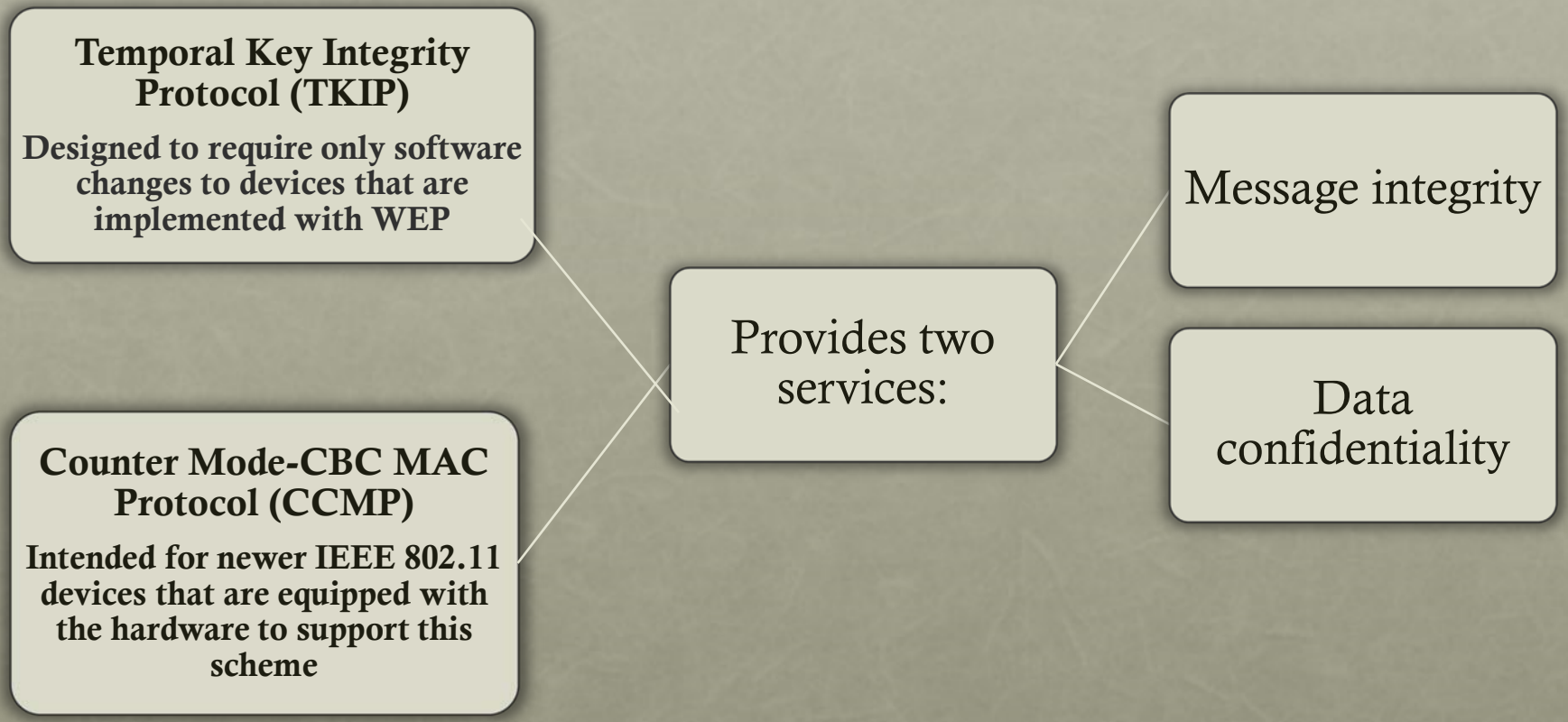


ELEMENTS OF IEEE 802.11i: Services and Corresponding Protocols



PROTECTED DATA TRANSFER PHASE

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

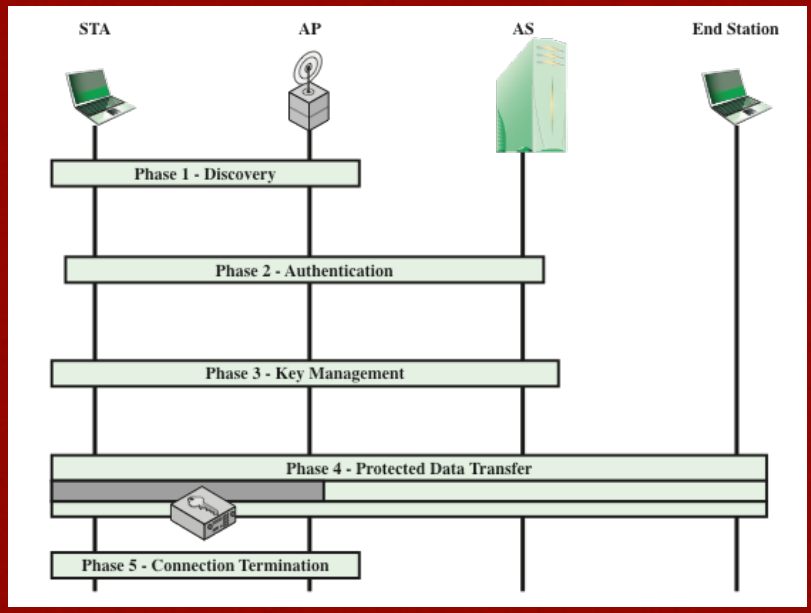


IEEE 802.11i Phases of Operation

- IEEE 802.11i security is concerned only with secure communication between the STA and its AP.

• Discovery:

- An AP uses messages called Beacons and Probe Responses to advertise its IEEE 802.11i security policy.
- The STA uses these to identify an AP for a WLAN with which it wishes to communicate.
- The STA associates with the AP, which it uses to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.

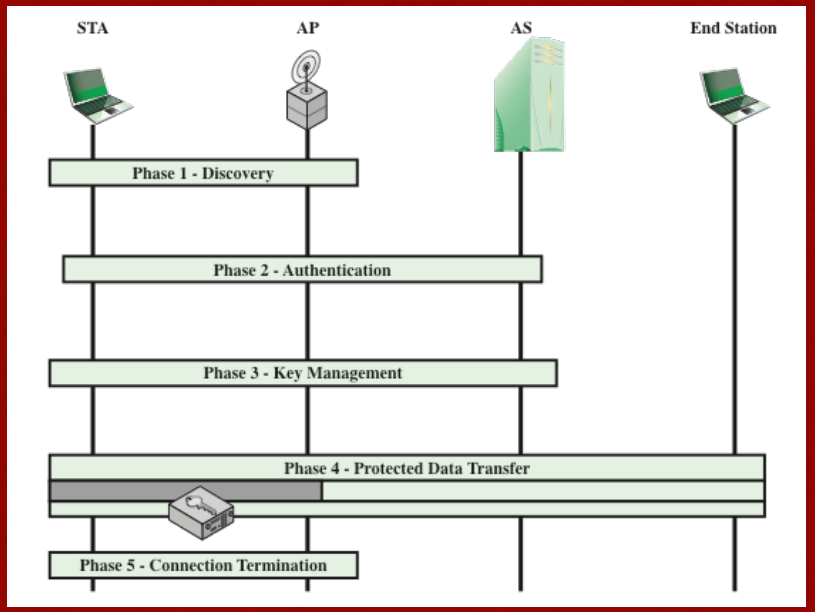


• Authentication:

- During this phase, the STA and AS prove their identities to each other.
- The AP blocks non-authentication traffic between the STA and AS until the authentication transaction is successful.
- The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.

IEEE 802.11i Phases of Operation

- IEEE 802.11i security is concerned only with secure communication between the STA and its AP.



• Key generation and distribution:
  - The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA.

• Protected data transfer:
  - Frames are exchanged between the STA and the end station through the AP.
  - As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.

• Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.

IEEE 802.11i Discovery and Association

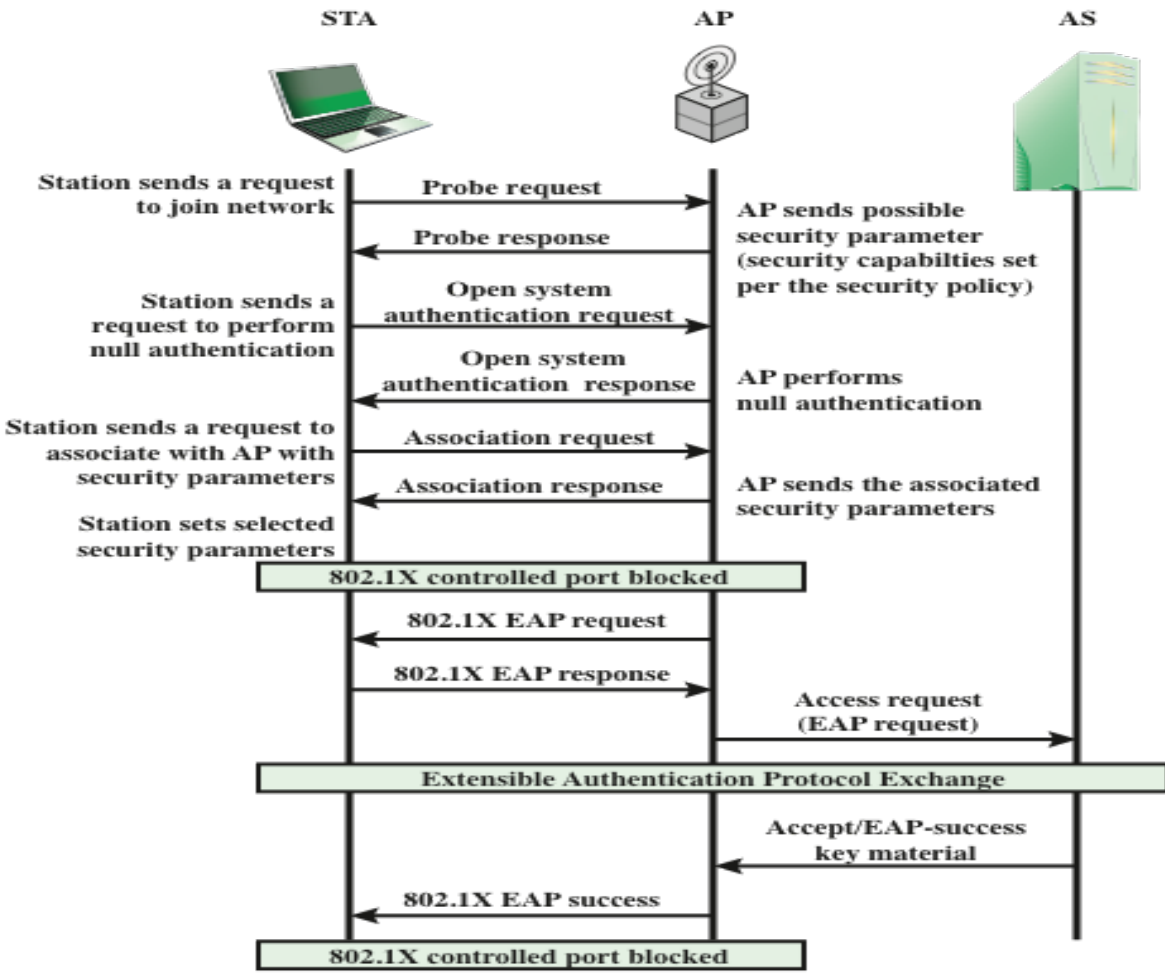


Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Associatio

Discovery and Association Step 1:

Discovery: Periodic Beacon signals from the AP or responds to a request from the STA

Security Capability (sets of possible suites):

- Confidentiality and integrity protocols
- The specification of a protocol with a key is called a **cipher suite**
- Authentication method
- Key management approach
- Another negotiable suite is Authentication and Key management **AKM**

Discovery and Association Step 2:

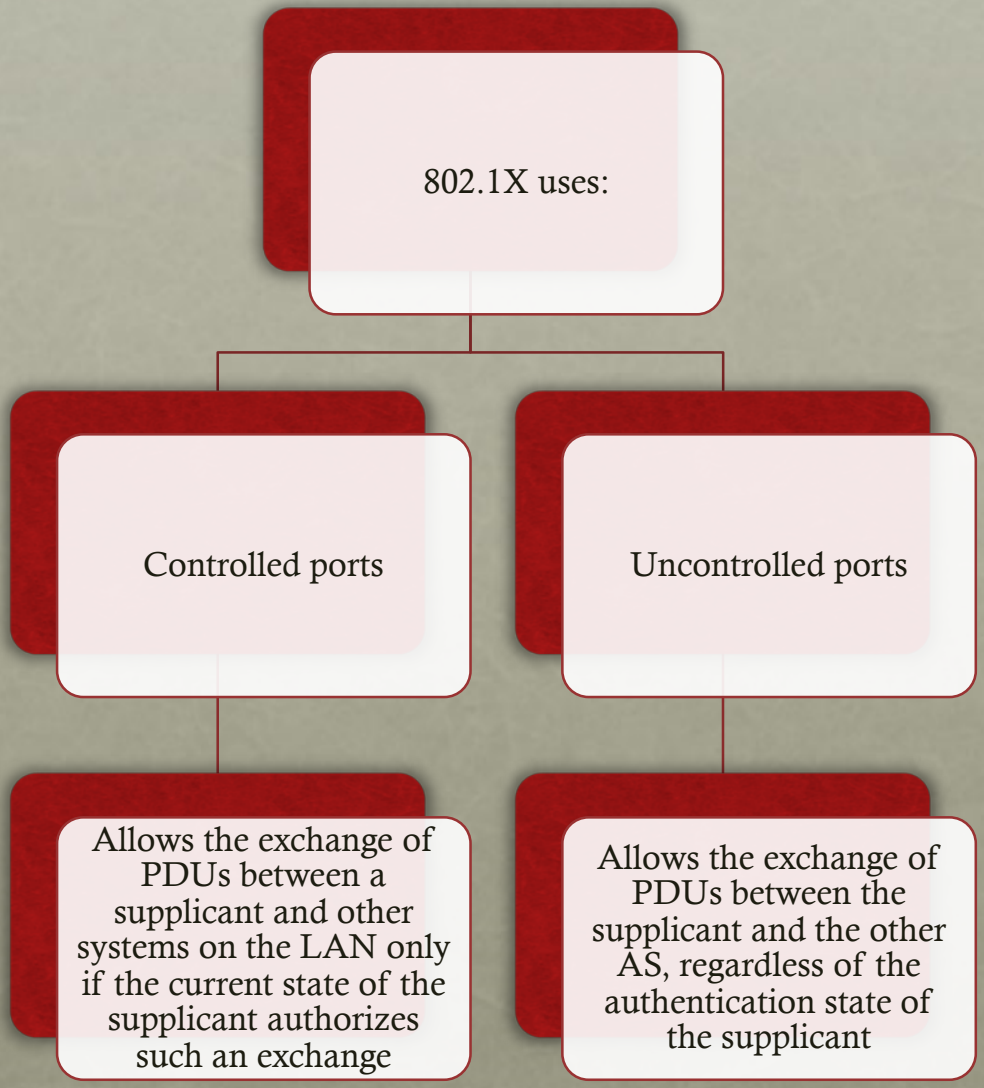
Null Authentication: for backward compatibility with 802.11 hardware

Discovery and Association Step 3:

Association: Agree on specific set of security capabilities (one specific cipher suite and one specific AKM suite)

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 is triggered right after the discovery phase to block user data and only allow authentication data to be transferred.



IEEE 802.11i Authentication Phase

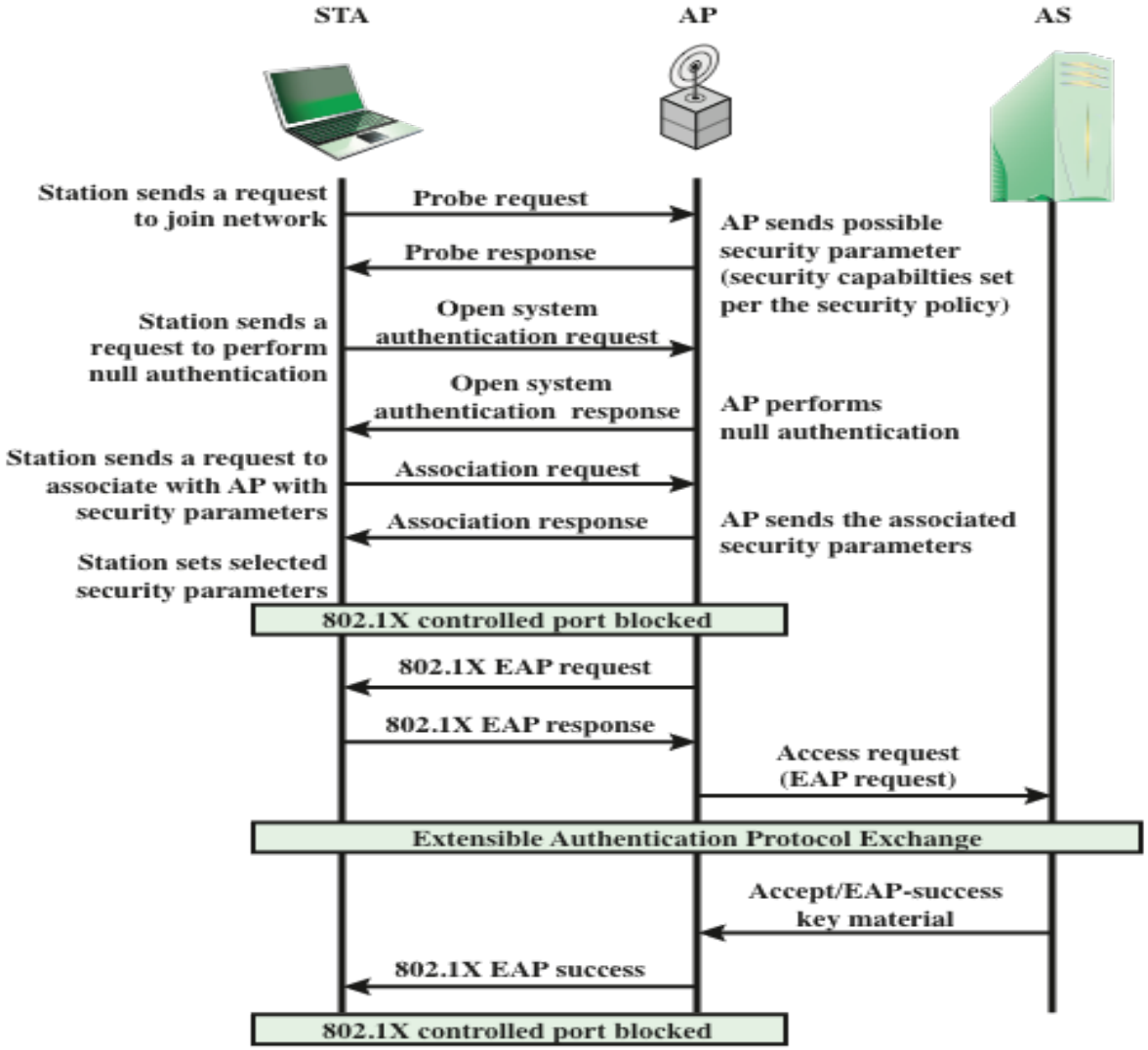


Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Associatio

Authentication phase:

- Designed to allow only authorized STAs to use the network and to provide STAs with assurance that it is communicating with a legitimate network
- Uses 802.1x Port based access control and EAPOL

Authentication Step 1: Connect to AS

- STA request from the AP for connection to AS.
- AP acknowledges the request and sends an access request to the AS

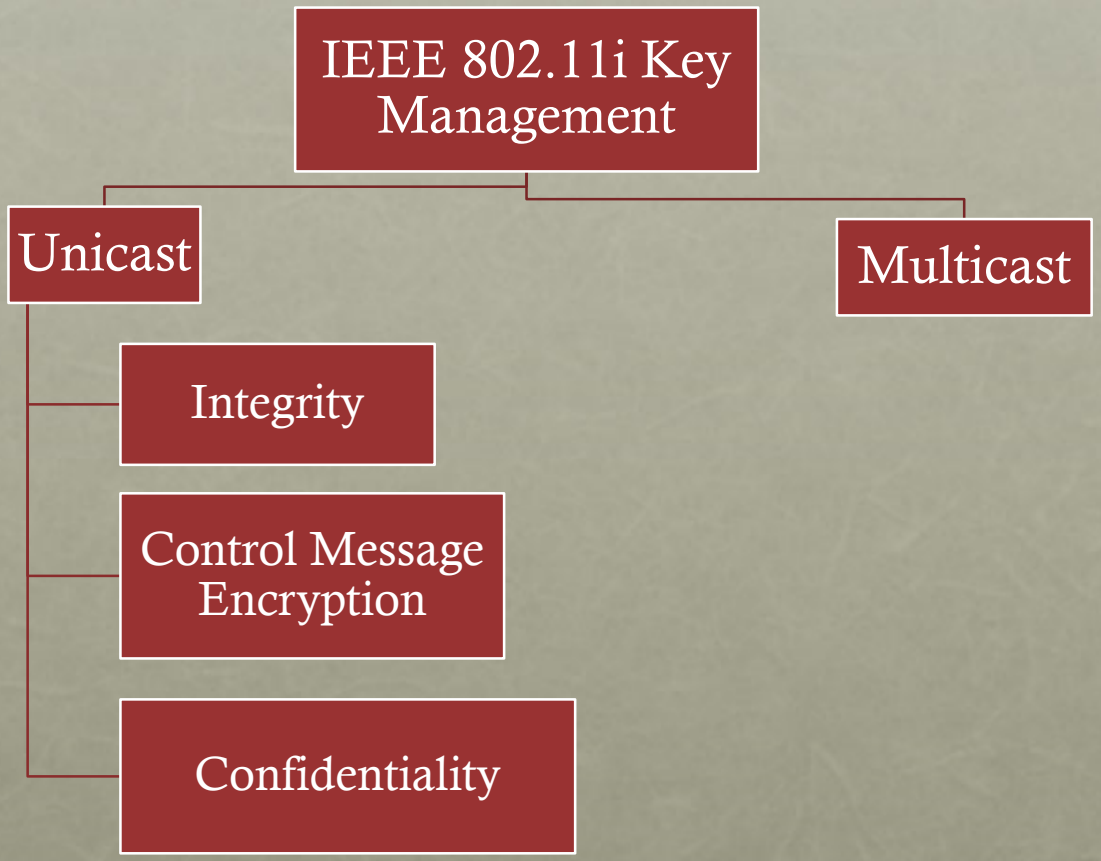
Authentication Step 2: EAP Exchange

- Exchange of authentication messages

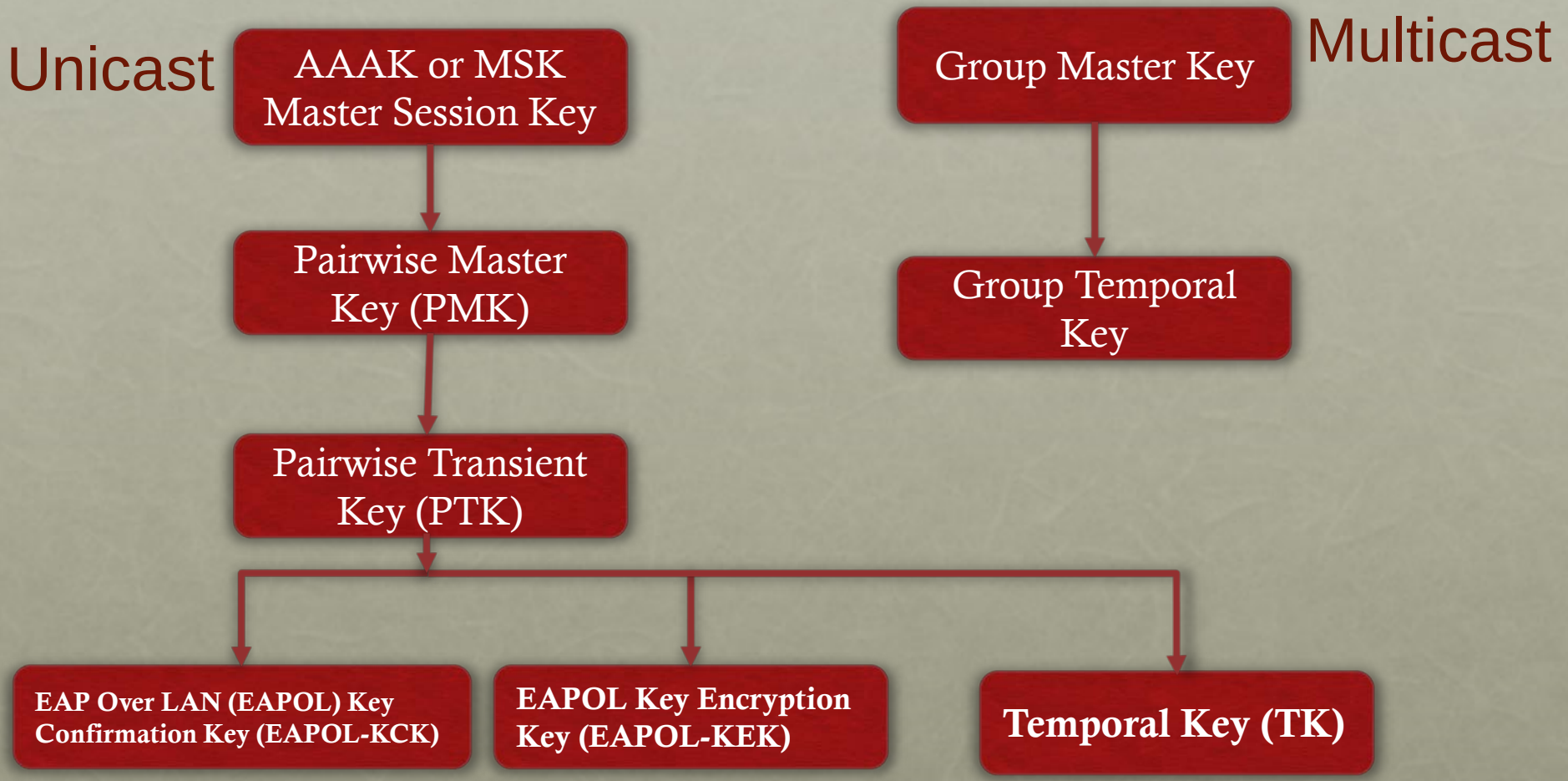
Authentication Step 3: Secure Key Delivery

- After authentication is successful, the AS generates a Master Session Key (MSK), also known as AAA Key (Authentication, Authorization and accounting)
- 802.11i relies on EAP for the secure delivery of the MSK

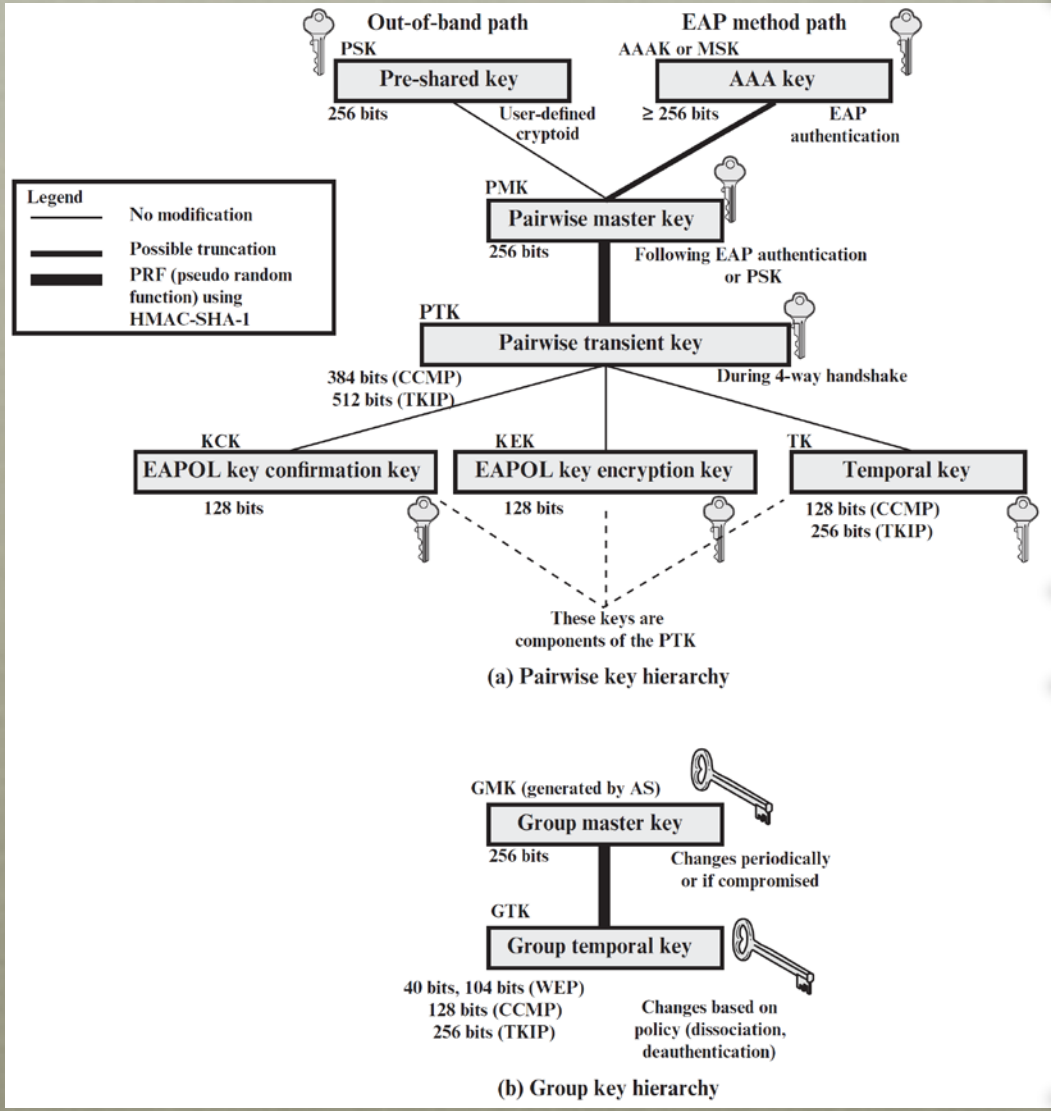
IEEE 802.11i KEY MANAGEMENT



KEY MANAGEMENT



KEY MANAGEMENT



Unicast

Multicast

4-WAY Handshake (Unicast):

1. AP → STA:
   - AP generates Anonce and sends it to the STA with its own MAC address
2. STA→ AP
   2.1 STA generates it own Snonce
   2.2 STA uses:
   - Snonce and
   - Anonce and
   - AP MAC address and
   - its own MAC Address and
   - PMK

   To generate PTK
   2.3 STA Hashes the:
   - Snonce and Its MAC Address using KCK
   - STA then sends the hashed message back to AP

3. AP → STA
   - AP is now able to generate same PTK
   - AP sends same message 1 above but including message integrity code
4. STA → AP: acknowledgment

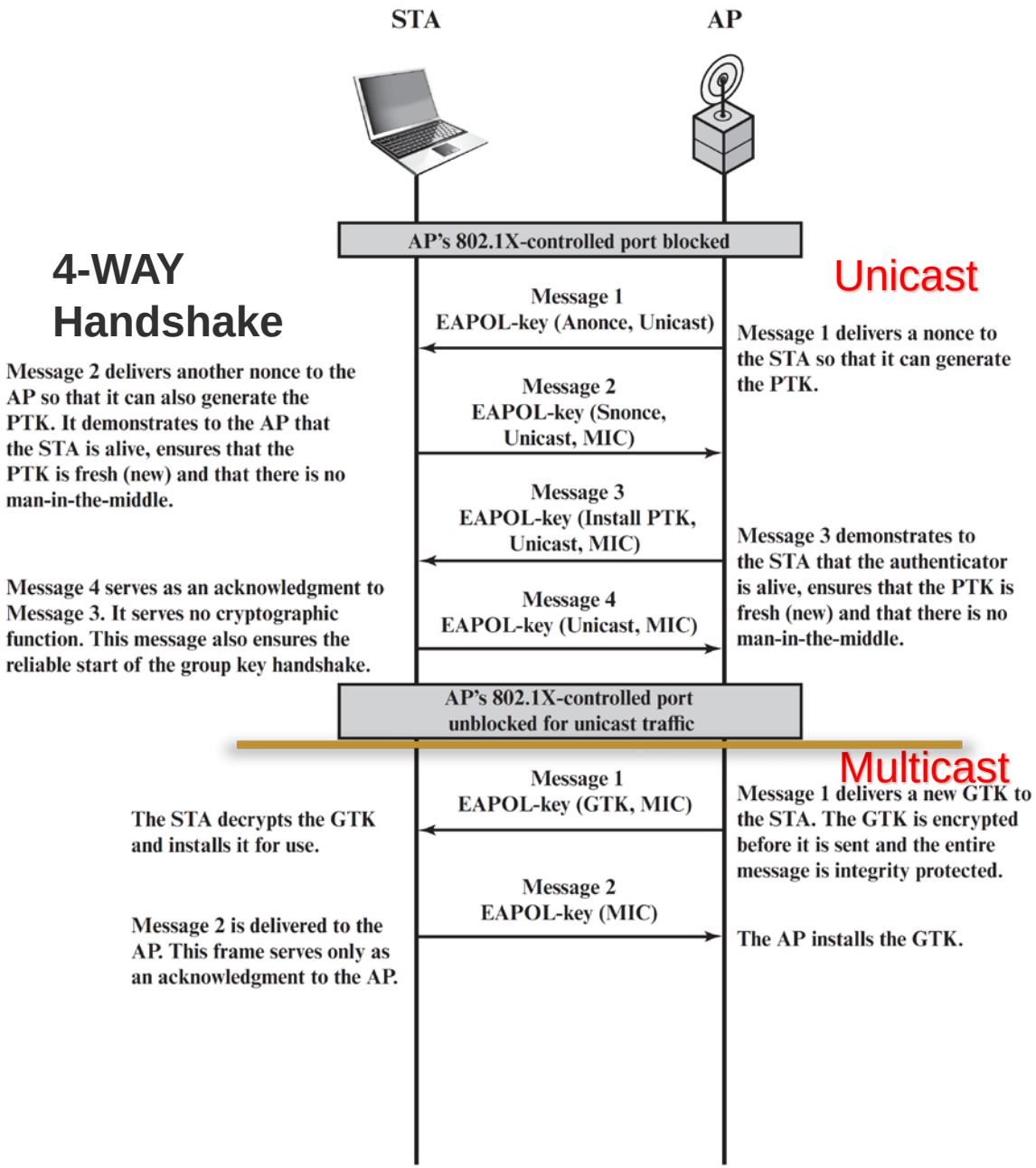


Figure 7.10 IEEE 802.11i Phases of Operation: 4-Way Handshake and Group Key Handshake

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

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 unicast 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. This is to prevent the device from receiving any more multicast or broadcast messages from the AP.

IEEE 802.11i KEYS & SUMMARY

By End of Phase 1:

- STA has discovered neighboring AP, and
- STA has associated itself with AP by selecting one method from the cipher suite and one method from AKM suite.
- Note: Null authentication is maintained for backward compatibility.
- At the end of Phase 1, 802.1x is triggered.

By End of Phase 2:

- The STA has authenticated itself with AS through AP.
- By the end of Authentication, AP and STA have received MSK and GMK.

By End of Phase 3:

- AP and STA use MSK and GMK to create PTK and GTK.

By End of Phase 4:

- STA use PTK and GTK to secure data transfer (confidentiality and integrity)

By End of Phase 5:

- Connection is terminated

Table 7.3 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

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

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