

CHAPTER - 6

WIRELESS NETWORK SECURITY



INTRODUCTION

- Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network.
- It is a subset of network security that adds protection for a wireless computer network.
- Wireless network security is also known as wireless security.



HOW IT WORKS?

- Wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default.
- Even if IT is compromised, the hacker is not able to view the content of the traffic/packet in transit.
- Moreover, wireless intrusion detection and prevention systems also enable protection by alerting the wireless network administrator in case of a security breach.
- Some of the common algorithms and standards to ensure wireless network security are Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA).



Why go wireless?

- The popularity of wireless network is clearly on the increase. But what are the hidden costs of going wireless? Are we giving up our security?
- The main **benefits** of wireless networking are:
 - cost
 - convenience
- The main **drawbacks** are:
 - speed
 - security



General Security Issues of Wireless Networks

- Network security issues, whether wired or wireless, fall into three main categories: availability, confidentiality and integrity:
- **Confidentiality:** is the information being sent across the network transmitted in such a way that only the intended recipient(s) can read it.
- **Integrity:** is the information reaching the recipient intact
- **Availability:** is the network available to users whenever it is supposed to be



Wi-Fi (Wireless Fidelity)

- **802.11**
- original 1997 2.4Ghz wireless Ethernet standard
- data rate 1 or 2Mbps
- **802.11a**
- 5Ghz frequency less susceptible to interference
- not compatible with 802.11b
- data rate of 54Mbps
- uses OFDM (Orthogonal Frequency Division Multiplexing)
- short range (60 feet)



Wi-Fi (Wireless Fidelity)

- **802.11b**
- most widely used standard
- up to 11Mbps
- 2.4Ghz frequency is subject to interference
- uses direct sequence spread spectrum modulation
- long range (300 feet)
- **802.11g**
- regarded by most as an extension to the life of 802.11b
- uses the OFDM bit of 802.11a and 2.4Ghz bit of 802.11b
- same frequency as 802.11b and so backwards compatible
- data rate of 54Mbps



Wi-Fi (Wireless Fidelity)

- **802.11i (coming soon)**
- IEEE certified security specification
- not a wireless protocol as such
- offers improved security for data in transit
- better control of who can use the network

- **802.11c/d/e/f/h/IR/j/k/m?**
- technical specifications of low level standards
- Gi-Fi (maybe coming, but not soon)
- theoretically 2Gbps can be achieved at frequencies of 56Ghz [1]



6.1 IEEE 802.11 WIRELESS LAN OVERVIEW


○ The Wi-Fi Alliance

- Wi-Fi is the brand given to 802.11 products certified by the Wi-Fi Alliance
- The first 802.11 standard to gain broad industry acceptance was 802.11b. Although 802.11b products are all based on the same standard, there is always a concern whether products from different vendors will successfully inter-operate
- To meet this concern, the Wireless Ethernet Compatibility Alliance (WECA), an industry consortium, was formed in 1999. This organization, subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance



6.1 IEEE 802.11 WIRELESS LAN OVERVIEW

○ The Wi-Fi Alliance

- This organization, subsequently renamed the Wi-Fi(Wireless Fidelity) Alliance, created a test suite to certify interoperability for 802.11b products.
 - The term used for certified 802.11b products is Wi-Fi.
 - Wi-Fi certification has been extended to 802.11g products.
 - The Wi-Fi Alliance has also developed a certification process for 802.11a products, called Wi-Fi5.
 - Recently, the Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards, referred to as Wi-Fi Protected Access (WPA).
 - The most recent version of WPA, known as WPA2, incorporates all of the features of the IEEE 802.11i WLAN security specification.
- 

IEEE 802.11 TERMINOLOGY

Table 6.1 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.



IEEE 802 PROTOCOL ARCHITECTURE

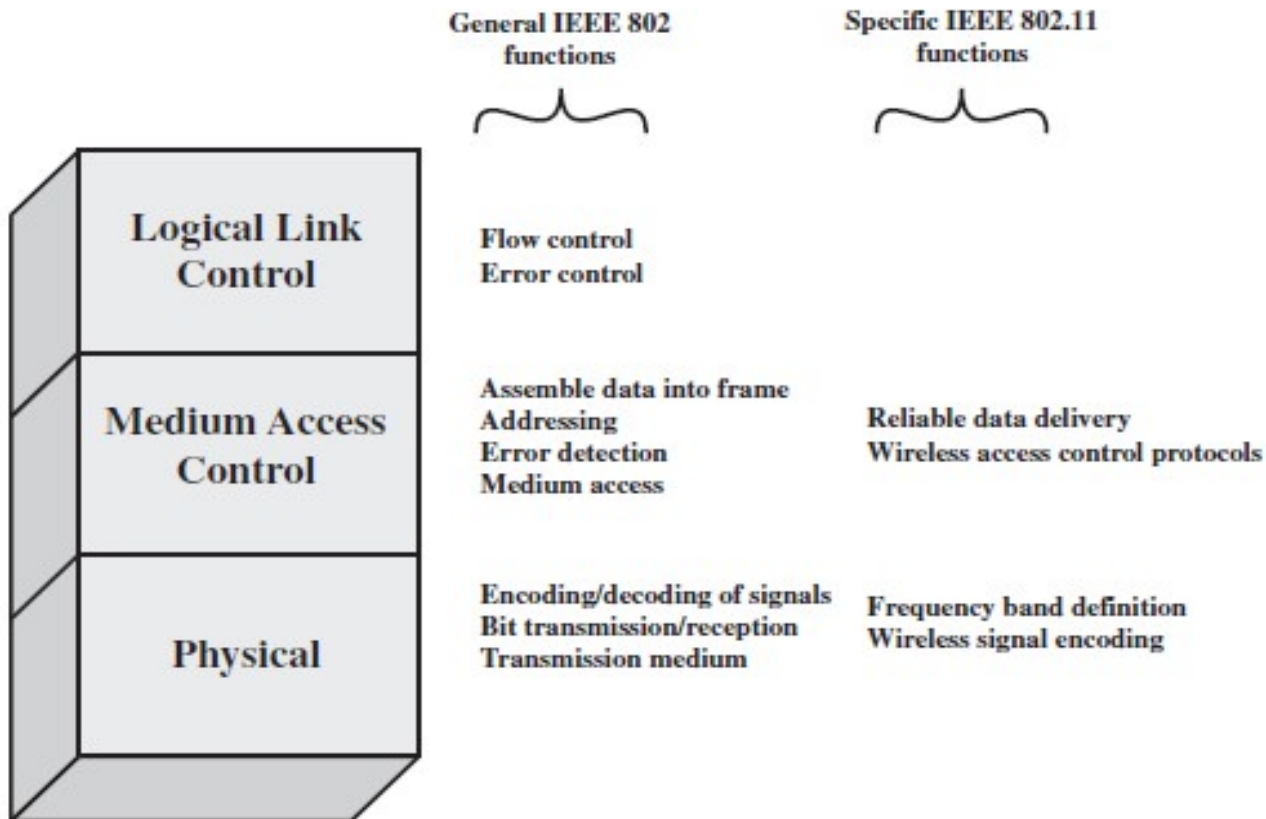


Figure 6.1 IEEE 802.11 Protocol Stack

❑ IEEE 802 PROTOCOL ARCHITECTURE

- IEEE 802.11 standards are defined within the structure of a layered set of protocols.
- This structure, used for all IEEE 802 standards, is illustrated in Figure 6.1.



□ IEEE 802 PROTOCOL ARCHITECTURE

○ ***PHYSICAL LAYER***

- IEEE 802 includes such functions as encoding /decoding of signals
- In the case of IEEE 802.11, the physical layer also defines frequency bands and antenna characteristics



CONTINUE...

○ **MEDIA ACCESS CONTROL**

- Devices in the same LAN share the network's transmission capacity.
- Media access control (MAC) layer provides controlled access to the transmission medium to provide an orderly and efficient use of that capacity.
- The MAC layer receives data from a higher-layer protocol, typically the Logical Link Control (LLC) layer, in the form of a block of data called **MAC service data unit (MSDU)**.
 - **MAC layer functions:** On transmission, assemble data into a frame, known as a MAC protocol data unit (MPDU) with address and error-detection fields.
 - On reception, disassemble frame, and perform address recognition and error detection.
 - Govern access to the LAN transmission medium.



□ IEEE 802 MPDU FORMAT

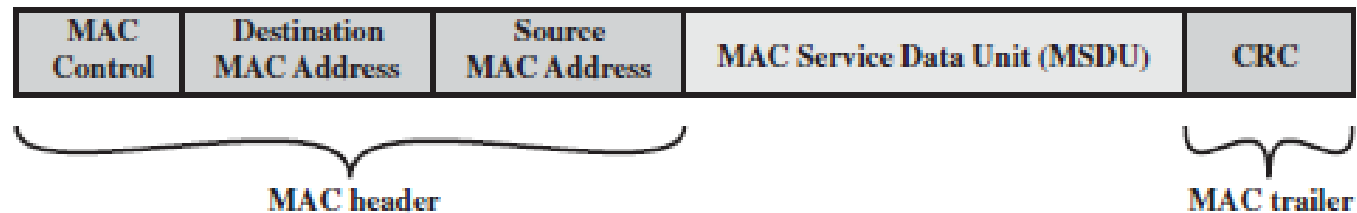


Figure 6.2 General IEEE 802 MPDU Format



CONTINUE...

The fields of this frame are as follows.

- **MAC Control:** This field contains any protocol control information needed for the functioning of the MAC protocol. For example, a priority level could be indicated here.
- **Destination MAC Address:** The destination physical address on the LAN for this MPDU.
- **Source MAC Address:** The source physical address on the LAN for this MPDU.
- **MAC Service Data Unit:** The data from the next higher layer.



CONTINUE...

- **CRC:** The cyclic redundancy check field; also known as the Frame Check Sequence (FCS) field.
- This is an error-detecting code, such as that which is used in other data-link control protocols.
- The CRC is calculated based on the bits in the entire MPDU. The sender calculates the CRC and adds it to the frame.
- The receiver performs the same calculation on the incoming MPDU and compares that calculation to the CRC field in that incoming MPDU.
- If the two values don't match, then one or more bits have been altered in transit.



CONTINUE...

- ***LOGICAL LINK CONTROL***

- Responsible for detecting errors using CRC and recovering from errors as well.
- In LAN protocol architecture these two functions are split between the MAC (for detecting errors) and LLC (for corecting errors)
- The LLC layer optionally keeps track of which frames have been successfully received and re-transmits unsuccessful frames.



❑ IEEE 802.11 NETWORK COMPONENTS AND ARCHITECTURAL MODEL

- The smallest building block of a wireless LAN is a basic service set (BSS), which consists of wireless stations.
- 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.
- In BSS, client stations don't communicate with each other directly but through AP and DS.
- A DS can be a switch, a wired network or a wireless network.



❑ IEEE 802.11 NETWORK COMPONENTS AND ARCHITECTURAL MODEL

- 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 ad hoc network.
- An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system.
- In an IBSS, the stations all communicate directly, and no AP is involved.
- An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system.
- The extended service set appears as a single logical LAN to the logical link control (LLC) level.



CONTINUE...

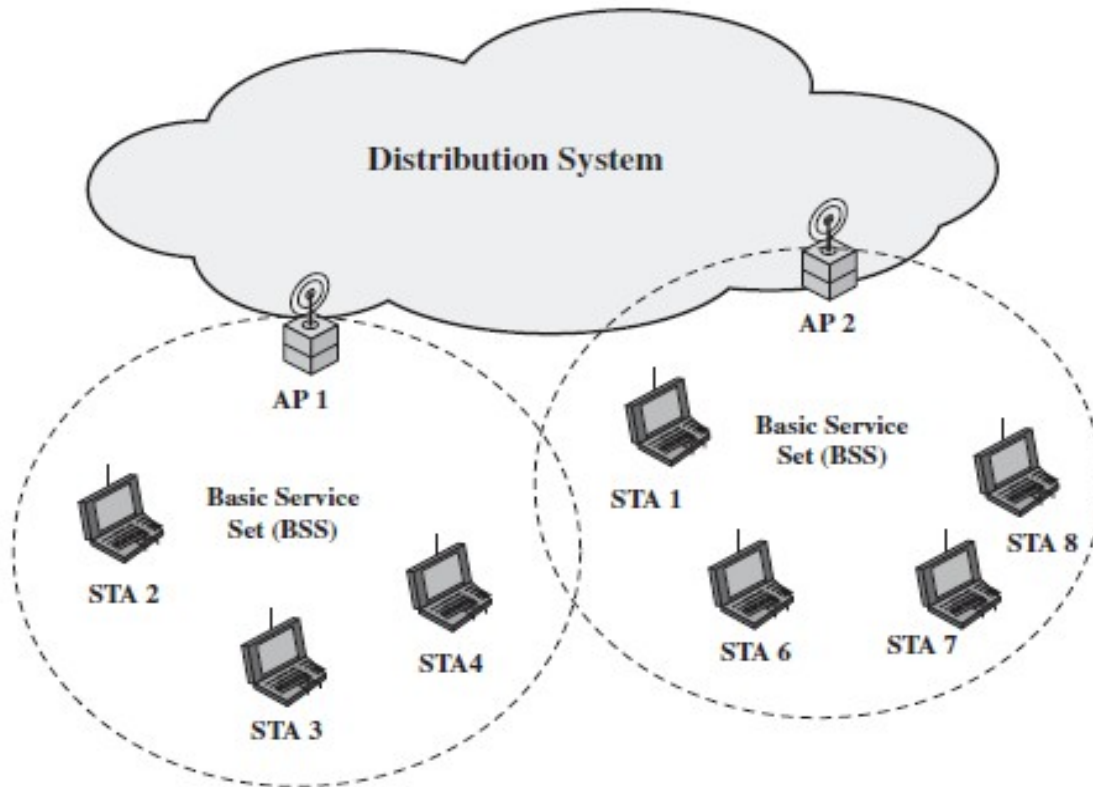


Figure 6.3 IEEE 802.11 Extended Service Set

A simple configuration is shown in Figure above, in which each station belongs to a single BSS; that is, each station is within wireless range only of other stations within the same BSS.

It is also possible for two BSSs to overlap geographically, so that a single station could participate in more than one BSS.

□ IEEE 802.11 SERVICES

- 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.
- Following Table lists the services and indicates two ways of categorizing them.



□ IEEE 802.11 SERVICES

- The service provider can be either the station or the DS. Station services are implemented in every 802.11 station, including AP stations.
- Distribution services are provided between BSSs; these services may be implemented in an AP or in another special-purpose device attached to the distribution system.
- **Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Six of the services are used to support delivery of MSDUs between stations.**
- If the MSDU is too large to be transmitted in a single MPDU, it may be fragmented and transmitted in a series of MPDUs.



□ IEEE 802.11 SERVICES

Table 6.2 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



□ IEEE 802.11 SERVICES

- **Distribution of messages within a DS** distribution and integration are used for distribution of messages.
- Distribution is the primary service to exchange MPDUs (between MAC layers) when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS.



□ IEEE 802.11 SERVICES

- For example, suppose a frame is to be sent from station 2 (STA 2) to station 7 (STA 7) in Figure 6.3. The frame is sent from STA 2 to AP 1, which is the AP for this BSS.
- The AP gives the frame to the DS, which has the job of directing the frame to the AP associated with STA 7 in the target BSS.
- AP 2 receives the frame and forwards it to STA 7. How the message is transported through the DS is beyond the scope of the IEEE 802.11 standard.
- If the two stations that are communicating are within the same BSS, then the distribution service logically goes through the single AP of that BSS.



□ IEEE 802.11 SERVICES

- **The integration service:** transfer of messages between IEEE 802.11 LAN and a station on an integrated IEEE802.x LAN
- Here integrated means a wired LAN connected to a DS and whose stations may be logically connected to the IEEE 803.11 LAN via integration service.
- **Association Related Services:** distribution service requires information about the stations within the ESS, which is provided by association related services.
- Before distribution service can deliver/accept data to and from a station, it must be associated.



□ IEEE 802.11 SERVICES

- The mobility standard defines three types of transitions based on mobility.
- **No transition:** A station is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.
- **BSS transition:** station movement from one BSS to another within the same ESS. Here, delivery of data to the station requires the addressing capability to recognize the new location of the station.
- **ESS transition:** Station movement from a BSS in one ESS to a BSS within another ESS. It is supported only if the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. In fact, disruption of service is likely to occur.



□ IEEE 802.11 SERVICES

- **Association Related Services:** To deliver a message within a DS, the distribution service needs to know where the destination station is located, the identity of the AP to deliver the message.
- For this the station must maintain an association with the AP within its current BSS. There are three services related to this:
- **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. A station should give this notification before leaving an ESS or shutting down.

□ IEEE 802.11i SERVICES

- Two characteristics of a wired LAN are not inherent in a wireless LAN.
- 1. In order to transmit over a wired LAN, a station must be physically connected to the LAN.
- On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit.
- There is a form of authentication with a wired LAN in that it requires some positive and presumably observable action to connect a station to a wired LAN.



□ IEEE 802.11i SERVICES

- 2. In order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN.
- On the other hand, with a wireless LAN, any station within radio range can receive.
- Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.



□ IEEE 802.11i SERVICES

- Differences between wired and wireless LANs suggest the increased need for robust security services and mechanisms for wireless LANs.
- The original 802.11 specification security features for privacy and authentication were quite weak.
- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.
- The final form of the 802.11i standard is referred to as **Robust Security Network (RSN)**.
- The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.



□ IEEE 802.11i SERVICES

- For privacy, 802.11 defined the Wired Equivalent Privacy (WEP) algorithm but it was weak.
- So to address the WLAN security issues, Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard.
- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard.
- The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.
- The final form of the 802.11i standard is referred to as **Robust Security Network (RSN)**.



6.2 IEEE 802.11i WIRELESS LAN SECURITY

- **IEEE 802.11i (RSN) Services**
- The 802.11i RSN security specification defines the following services.
- **Authentication:** A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.

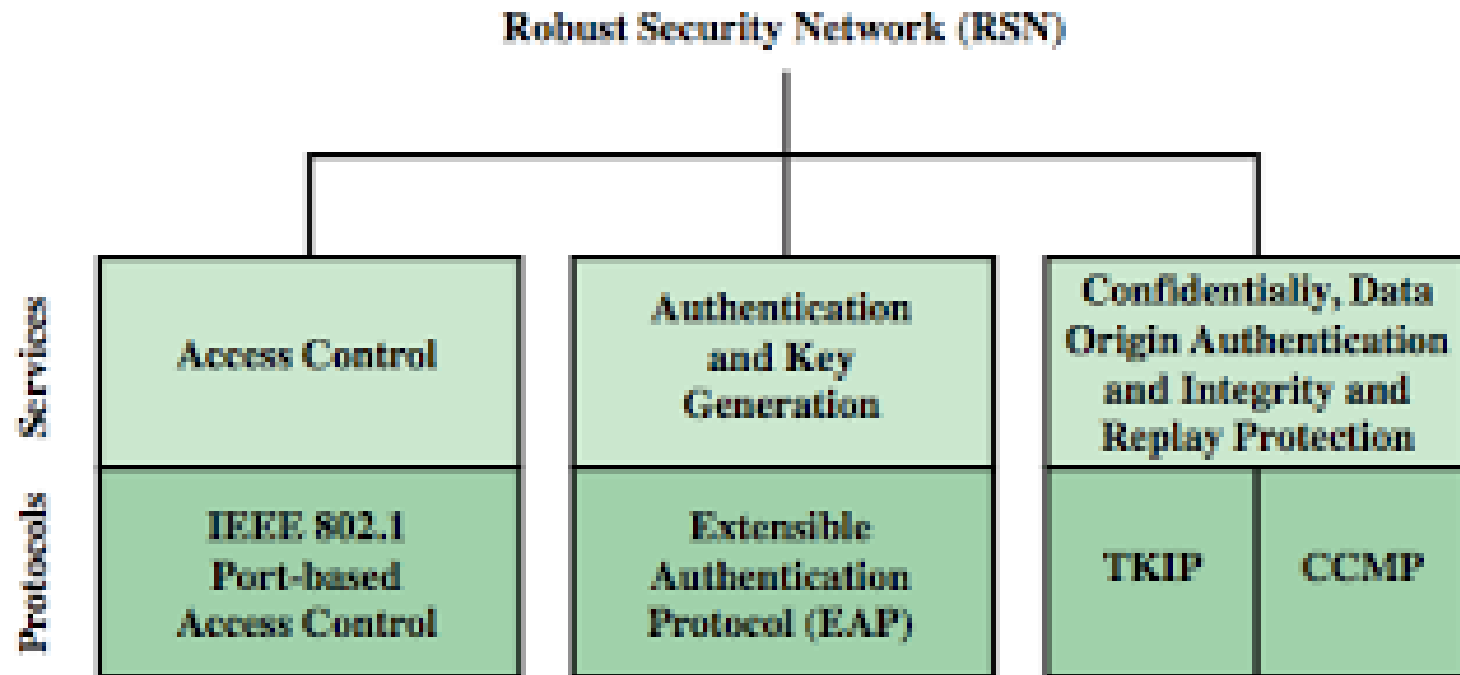


6.2 IEEE 802.11I WIRELESS LAN SECURITY

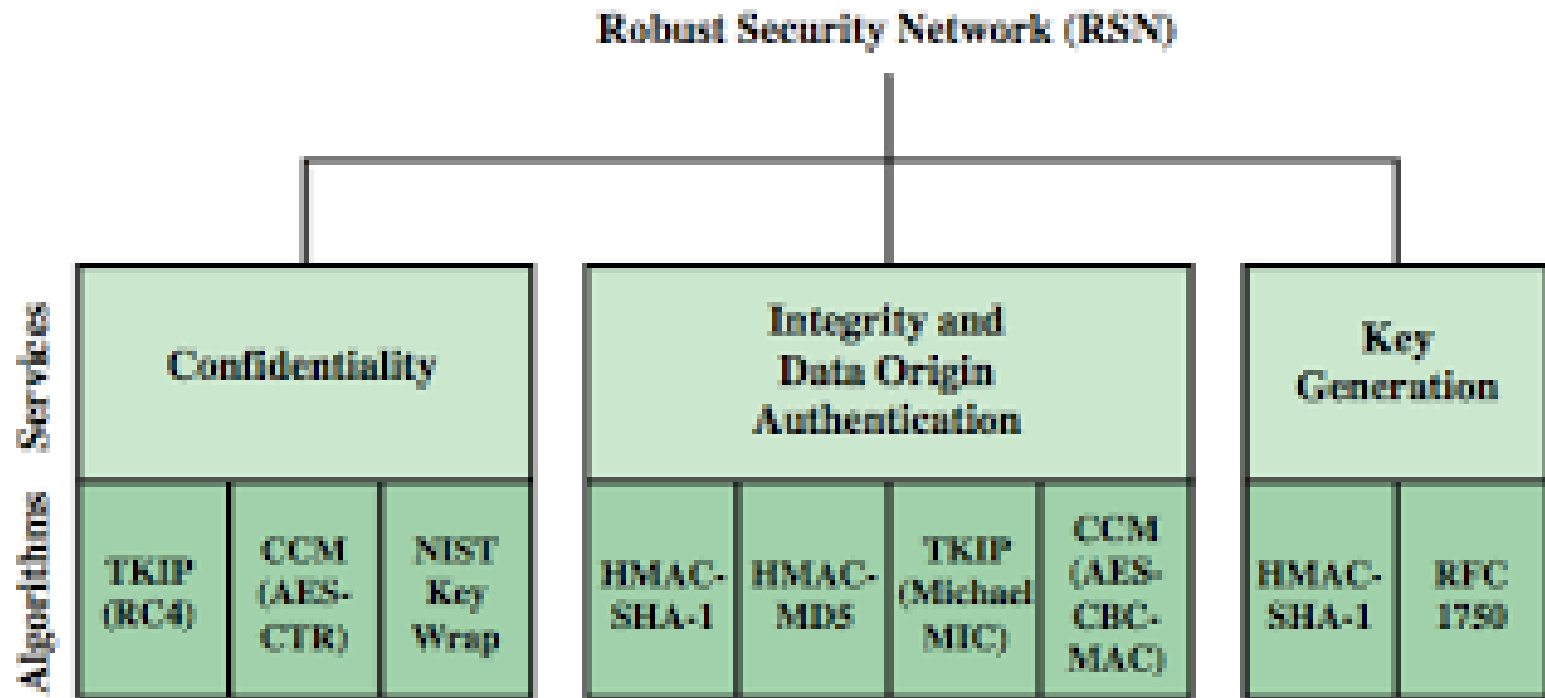
- **Access control:** This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.
- **Privacy with message integrity:** MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered.



Services and protocols



Cryptographic Algorithms



❑ IEEE 802.11i Phases of Operation

- The operation of an IEEE 802.11i RSN can be broken down into five distinct phases of operation.
- The exact nature of the phases will depend on the configuration and the end points of the communication. Possibilities include:
 - 1. Two wireless stations in the same BSS communicating via the access point (AP) for that BSS.
 - 2. Two wireless stations (STAs) in the same ad hoc IBSS communicating directly with each other.
 - 3. Two wireless stations in different BSSs communicating via their respective APs across a distribution system.
 - 4. A wireless station communicating with an end station on a wired network via its AP and the distribution system.



❑ IEEE 802.11i Phases of Operation

- In case 1 security is provided ensuring secure communication between station and AP
- In case 2 AP functionality is resided in station itself.
- In case 3 security is not provided across DS but only within each BSS.
- In case 4 too the security is provided between the AP and the station.



IEEE 802.11i PHASES OF OPERATION

Following figure shows how five phases of RSN operations are mapped with network components involved. One new component is the authentication server (AS). The rectangles indicate the exchange of sequences of MPDUs

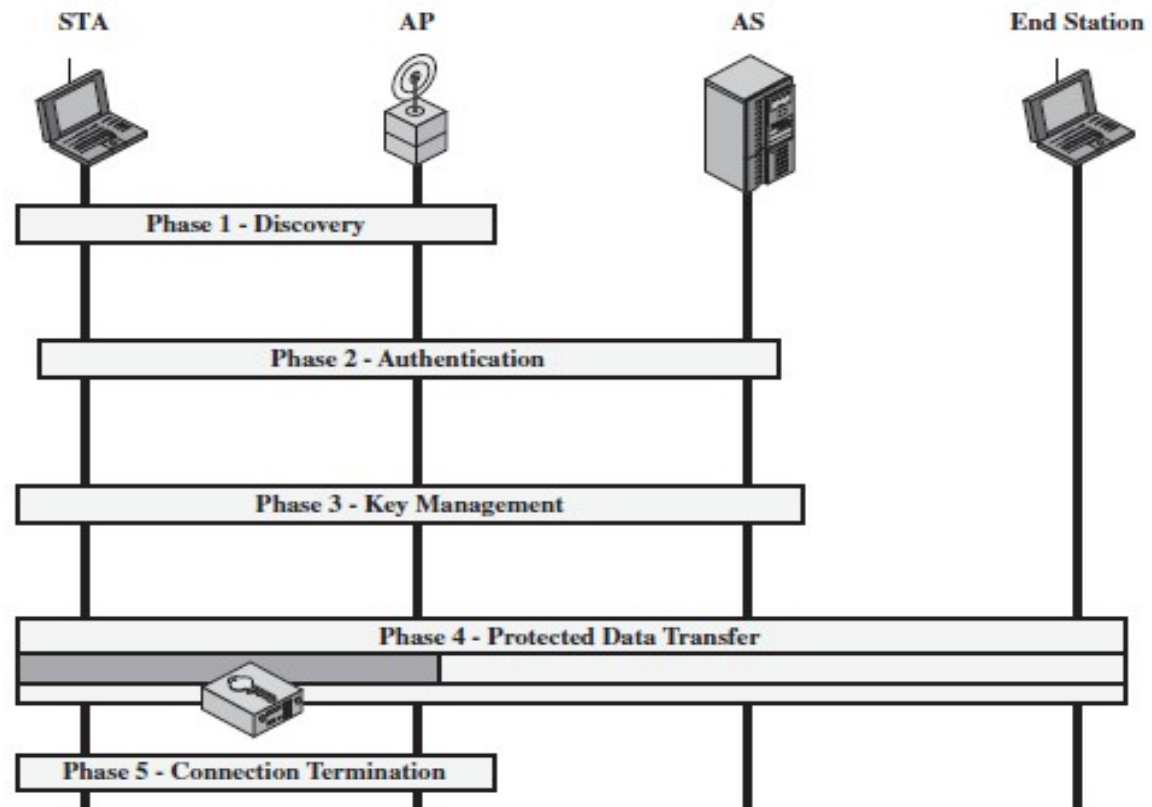


Figure 6.5 IEEE 802.11i Phases of Operation

❑ IEEE 802.11i Phases of Operation

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.



❑ IEEE 802.11i Phases of Operation

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.

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.

Frames are exchanged between the AP and STA only.



❑ IEEE 802.11i Phases of Operation

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.



CONTINUE...

- **Discovery:**

- *SECURITY CAPABILITIES:*

- *During this phase, the STA and AP decide on specific techniques in the following areas:*

- Confidentiality and MPDU integrity protocols for protecting unicast traffic
 - Authentication method
 - Cryptography key management approach



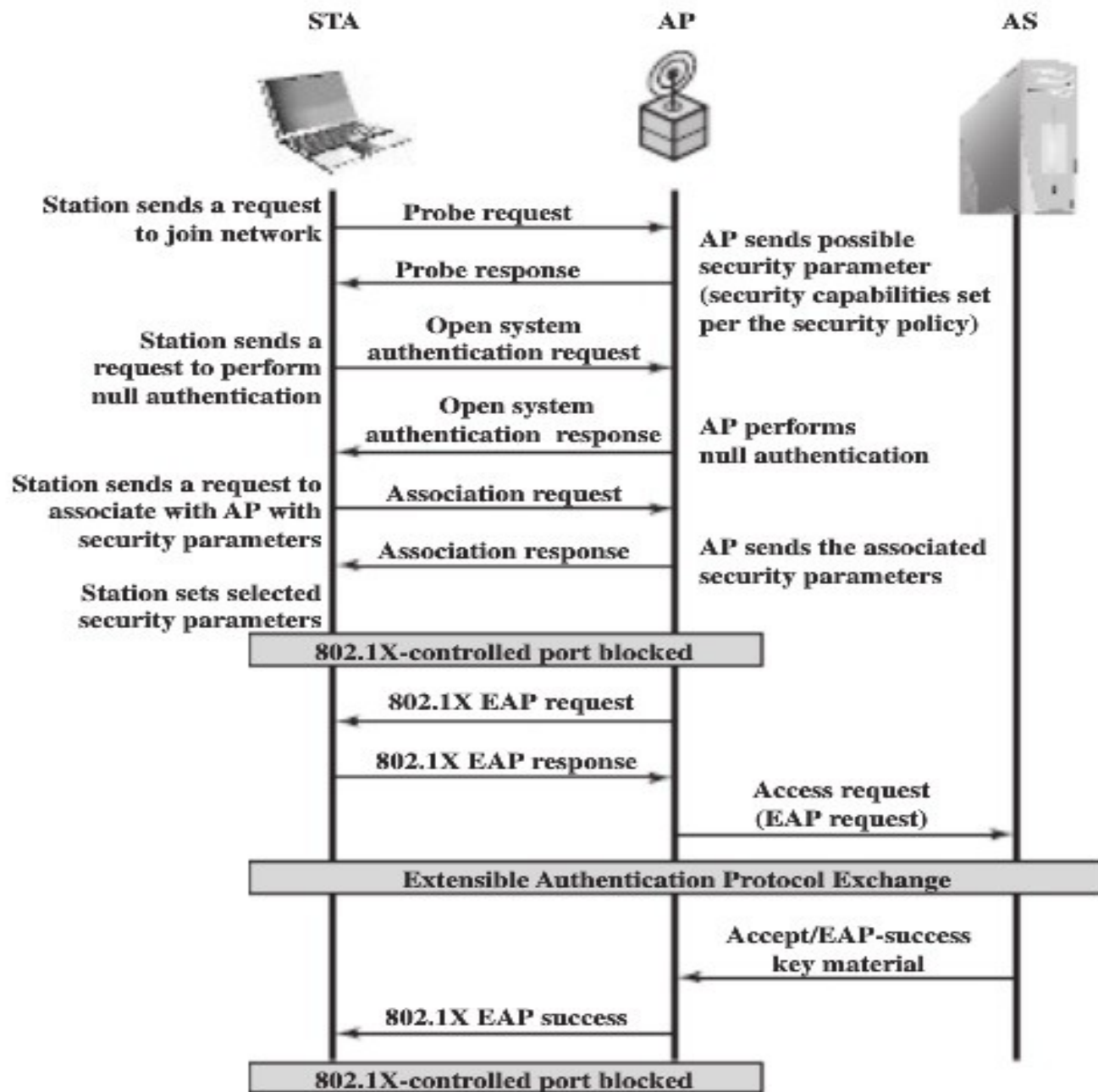


Figure 7.8 IEEE 802.11i Phases of Operation: Capability Discovery, Authentication, and Association

CONTINUE...

○ ***MPDU EXCHANGE***

● **Network and security capability discovery:**

- During this exchange, STAs discover the existence of a network with which to communicate
- The AP either periodically broadcasts its security capabilities in a specific channel through the Beacon frame; or responds to a station's Probe Request through a Probe Response frame



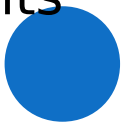
CONTINUE...

○ ***MPDU EXCHANGE***

● **Open system authentication:**

- The two devices (STA and AP) simply exchange identifiers.
- It provides no security

● **Association:**


- The purpose of this stage is to agree on a set of security capabilities to be used. The STA then sends an Association Request frame to the AP
 - If there is no match in capabilities between the AP and the STA, the AP refuses the Association Request.
 - The STA blocks it too, in case it has associated with a rogue AP or someone is inserting frames illicitly on its channel.
- 

CONTINUE...

○ **Authentication Phase**

- Allows only authorized stations to use the network and to provide the STA with assurance of being a legitimate network.

○ **IEEE 802.1X ACCESS CONTROL APPROACH**

- IEEE 802.11i uses a standard to provide access control functions for LANs - IEEE 802.1X, Port-Based Network Access Control.
 - The authentication protocol - the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard.
 - IEEE 802.1X uses the terms *supplicant*(wireless station), *authenticator*(AP), and *authentication server (AS)*.
 - Here AS is typically a separate device on the wired side of the network (i.e., accessible over the DS) but could also reside directly on the authenticator.
- 

CONTINUE...

- Before a supplicant is authenticated, it can only pass control or authentication messages between the supplicant and the AS; *the 802.1X control channel is unblocked, but the 802.11 data channel is blocked.*
- As indicated in Figure 6.7, 802.1X uses controlled and uncontrolled ports.
- Ports are logical entities defined within the authenticator and refer to physical network connections
- For a WLAN, the authenticator (the AP) may have only two physical ports: one connecting to the DS and one for wireless communication within its BSS.
- Each logical port is mapped to one of these two physical ports.



CONTINUE...

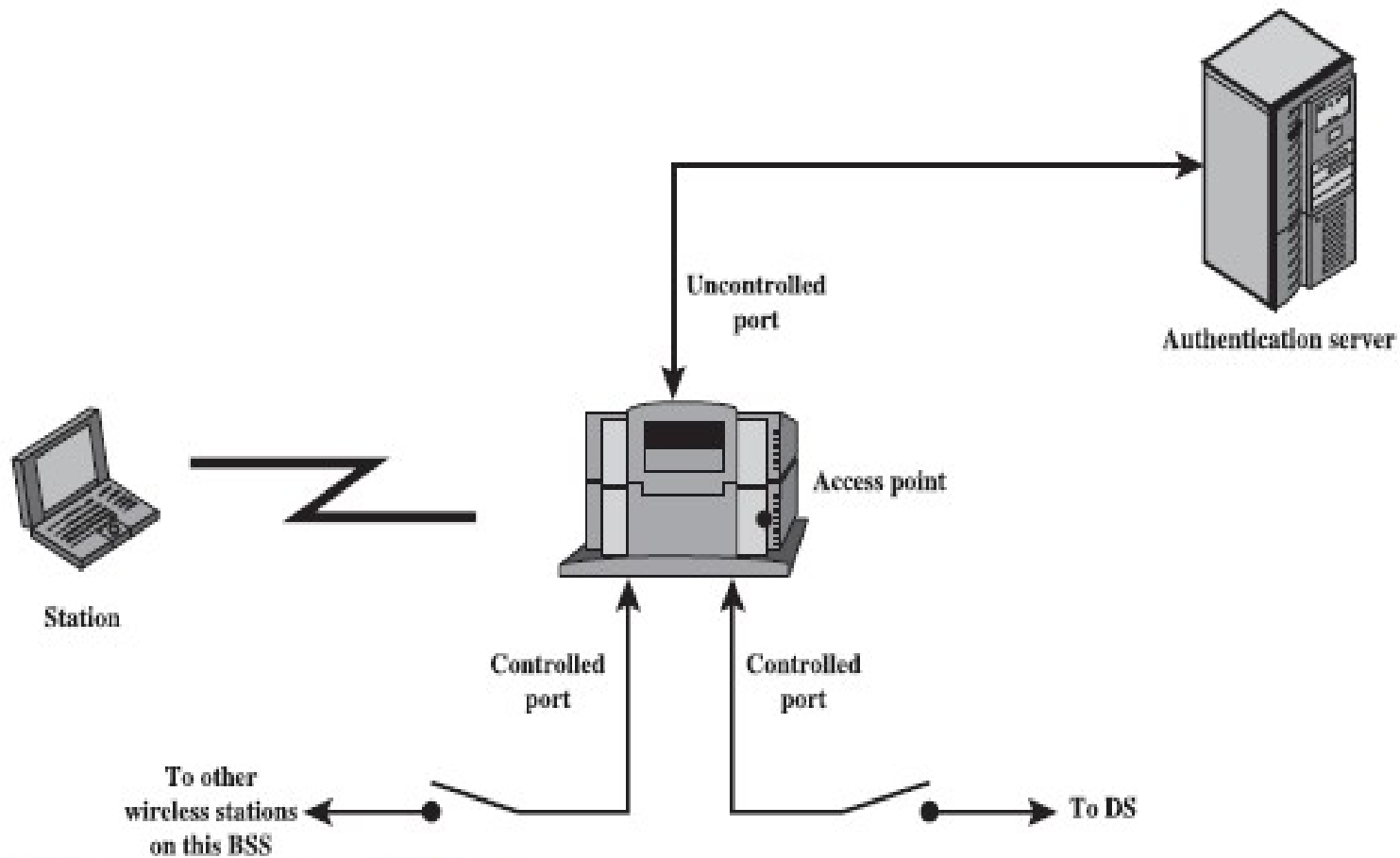


Figure 6.7 802.1X Access Control



CONTINUE...

- An **uncontrolled port** allows the exchange of PDUs between the supplicant and the other AS, regardless of the authentication state of the supplicant.
- A **controlled port** 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.



CONTINUE...

- The 802.1X framework, with an upper-layer authentication protocol, fits nicely with a BSS architecture that includes a number of wireless stations and an AP.
- For an IBSS, there is no AP. For an IBSS, 802.11i provides a more complex solution that, in essence, involves pair wise authentication between stations on the IBSS.



CONTINUE...

○ **MPDU EXCHANGE**

- The lower part of Figure 6.6 shows the MPDU exchange dictated by IEEE 802.11 for the authentication phase.
- **Connect to AS:**
 - The STA sends a request to its AP (the one with which it has an association) for connection to the AS.
 - The AP acknowledges this request and sends an access request to the AS.
- **EAP exchange: (Extensible Authentication Protocol)**
 - This exchange authenticates the STA and AS to each other.



CONTINUE...

- **Secure key delivery:**

- Once authentication is established, the AS generates a master session key (MSK), also known as the Authentication, Authorization, and Accounting (AAA) key and sends it to the STA.
- All the cryptographic keys needed by the STA for secure communication with its AP are generated from this MSK.
- IEEE 802.11i does not prescribe a method for secure delivery of the MSK but relies on EAP.
- Whatever method is used, it involves the transmission of an MPDU containing an encrypted MSK from the AS, via the AP, to the AS.



CONTINUE...

○ **EAP EXCHANGE**

- Typically, the message flow between STA and AP employs the EAP over LAN (EAPOL) protocol, and the message flow between the AP and AS uses the Remote Authentication Dial In User Service (RADIUS) protocol
 - The EAP exchange begins with the AP issuing an EAP-Request/Identity frame to the STA.
 - The STA replies with an EAP-Response/Identity frame to AP. The packet is then encapsulated in RADIUS over EAP and passed on to the RADIUS server as a RADIUS-Access-Request packet.
 - The AAA server replies with a RADIUS-Access-Challenge packet, which is passed on to the STA as an EAP-Request
 - The STA formulates an EAP-Response message and sends it to the AS.
 - The AAA server grants access with a Radius-Access-Accept packet. The AP issues an EAP-Success frame.



CONTINUE...

○ **Key Management Phase**

- During the key management phase, a variety of cryptographic keys are generated and distributed to STAs.
- There are two types of keys:
 - **Pairwise keys** used for communication between an STA and an AP
 - **Group keys** used for multicast communication.



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

Table 6.3
IEEE 802.11i
Keys for Data
Confidentiality and
Integrity Protocols



CONTINUE...

○ PAIRWISE KEYS

- Pair wise keys are used for communication between a pair of devices, typically between an 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.
- At the top two possibilities: PSK (Pre-Shared Key) a secret key shared by AP and STA not managed by IEEE 802.11i. The other key is Master Session Key(MSK), created with IEEE 802.X protocol.
- The method of key generation is specific to authentication protocol.
- In any case, a unique key is shared by AP to STA for communication.



CONTINUE...

○ PAIRWISE KEYS

- All other keys derived from the master key
- Each STA has a set of keys as shown in figure and AP has set of keys for each STA.
- The PMK is derived from the master key.
- If PSK is used, then PSK is used as PMK. If MSK is used, then PMK is derived by truncating MSK
- PMK is used to generate PTK, which consists of three keys and derived using HMAC-SHA-1 function with MAC addresses of AP and STA
- Three parts of PTK are as follows:
- Temporal Key (TK): Provides the actual protection for user traffic.



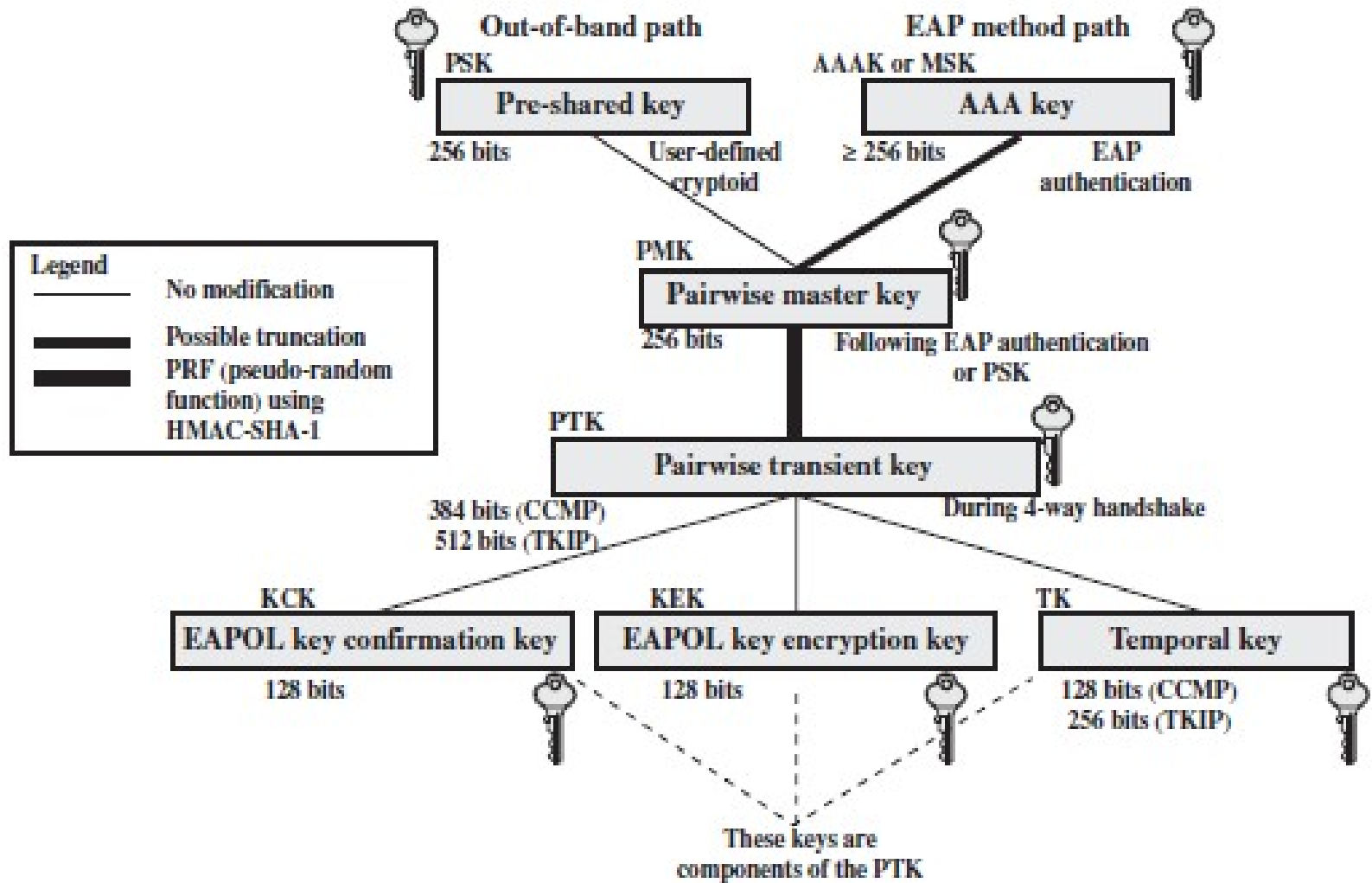
CONTINUE...

○ PAIRWISE KEYS

- 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.



CONTINUE...



(a) Pairwise key hierarchy

CONTINUE...

○ **PAIRWISE KEY DISTRIBUTION**

- This exchange is known as the 4-way handshake.
 - **AP->STA:** Message includes the MAC address of the AP and a nonce
 - **STA->AP:** The STA generates its own nonce (Snonce) and uses both nonces and both MAC addresses, plus the PMK, to generate a PTK. The STA then sends a message containing its MAC address and Snonce, enabling the AP to generate the same PTK.
 - **AP->STA:** The AP is now able to generate the PTK. The AP then sends a message to the STA, containing the same information as in the first message, but this time including a MIC(Message Integrity Code).
 - **STA->AP:** This is merely an acknowledgment message.



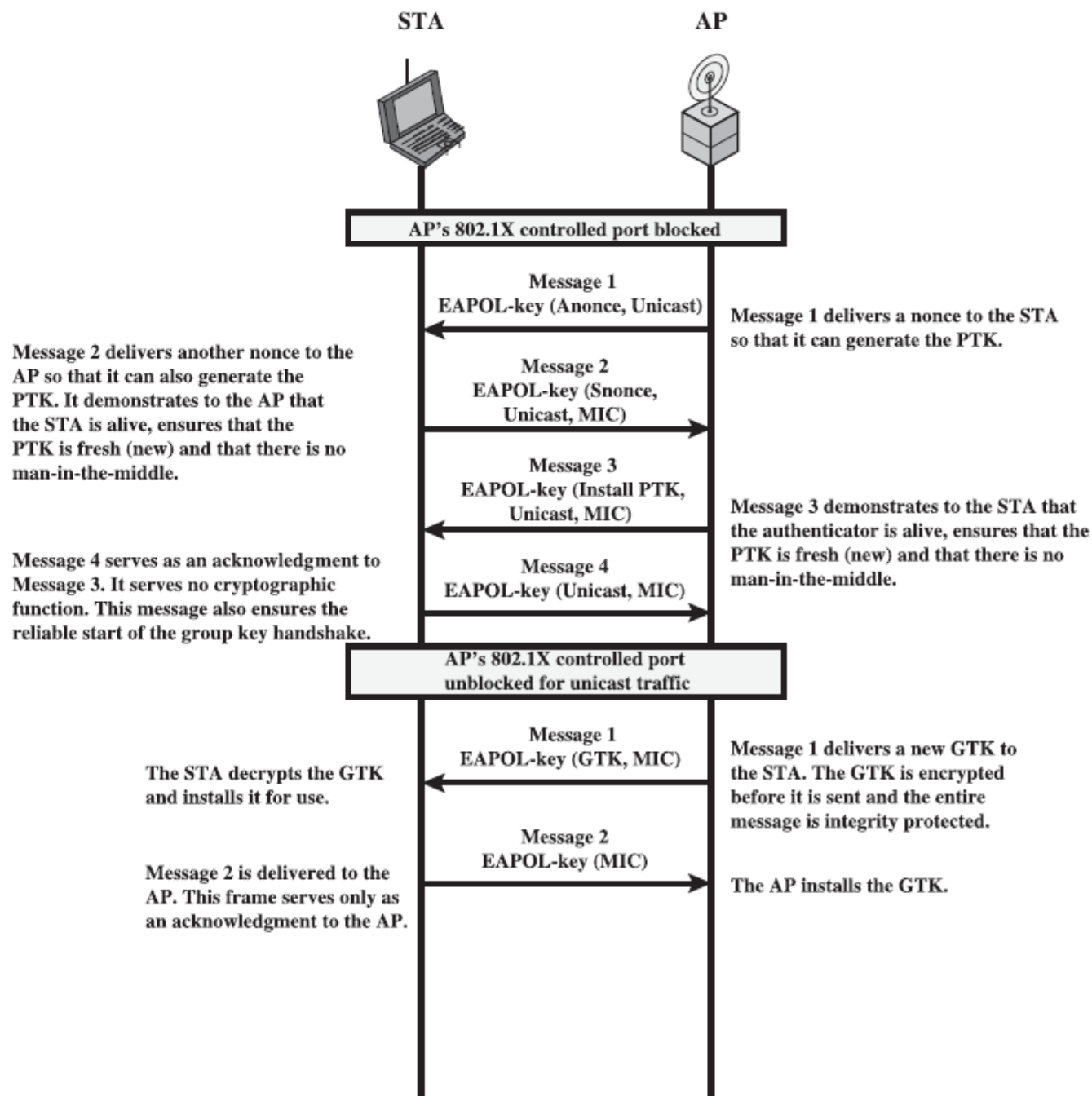


Figure 6.9 IEEE 802.11i Phases of Operation: Four-Way Handshake and Group Key Handshake

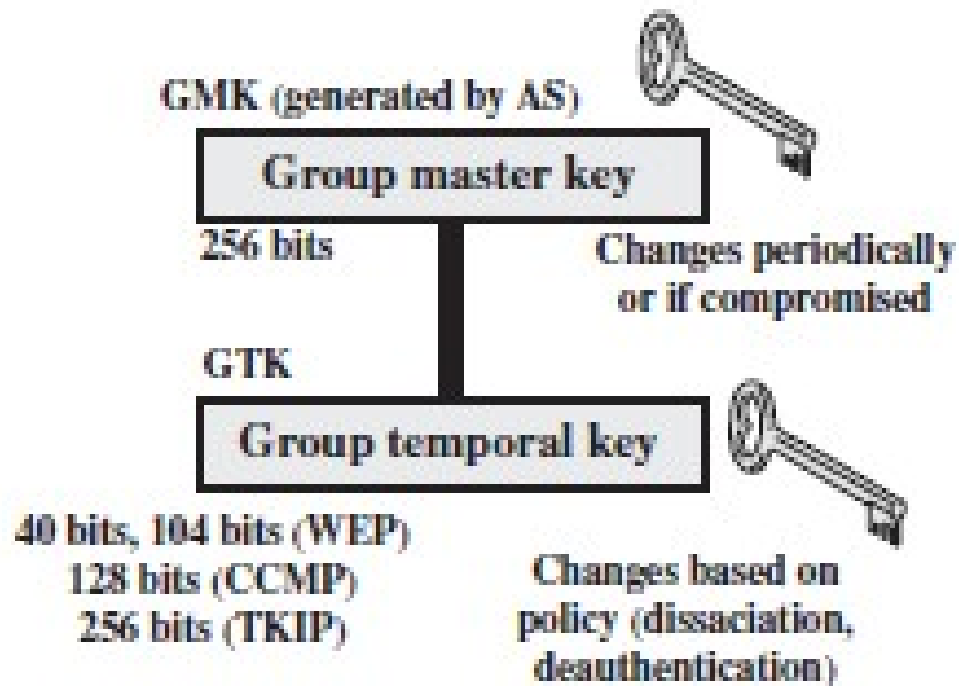
CONTINUE...

- **GROUP KEYS**

- Group keys are used for multicast communication in which one STA sends MPDU's to multiple STAs.



CONTINUE...



(b) Group key hierarchy



CONTINUE...

- **GROUP KEY DISTRIBUTION**
- **AP->STA:** This message includes the GTK, encrypted either with RC4 or with AES. The key used for encryption is KEK. A MIC value is appended.
- **STA->AP:** The STA acknowledges receipt of the GTK. This message includes a MIC value.



CONTINUE...

○ Protected Data Transfer Phase

- IEEE 802.11i defines two schemes for protecting data transmitted in 802.11 MPDUs: the Temporal Key Integrity Protocol (TKIP), and the Counter Mode-CBC MAC Protocol (CCMP).

○ ***TKIP***

- TKIP provides two services
 - Message integrity
 - Data confidentiality

○ ***CCMP***

- CCMP provides two services
 - Message integrity
 - Data confidentiality



❑ THE IEEE 802.11i PSEUDORANDOM FUNCTION

- At a number of places in the IEEE 802.11i scheme, a pseudorandom function (PRF) is used. For example, it is used to generate nonces, to expand pairwise keys, and to generate the GTK.
- The IEEE 802.11i PRF takes four parameters as input and produces the
- desired number of random bits. The function is of the form $\text{PRF}(K, A, B, \text{Len})$, where
- K = a secret key
- A = a text string specific to the application
- B = some data specific to each case
- Len = desired number of pseudorandom bits



CONTINUE...

- For example, for the pairwise transient key for CCMP:
 - $PTK = PRF(PMK, \text{"Pairwise key expansion"}, \min(AP\text{-}Addr, STA\text{-}Addr) || \max(AP\text{-}Addr, STA\text{-}Addr) || \min(Anonce, Snonce) || \max(Anonce, Snonce), 384)$

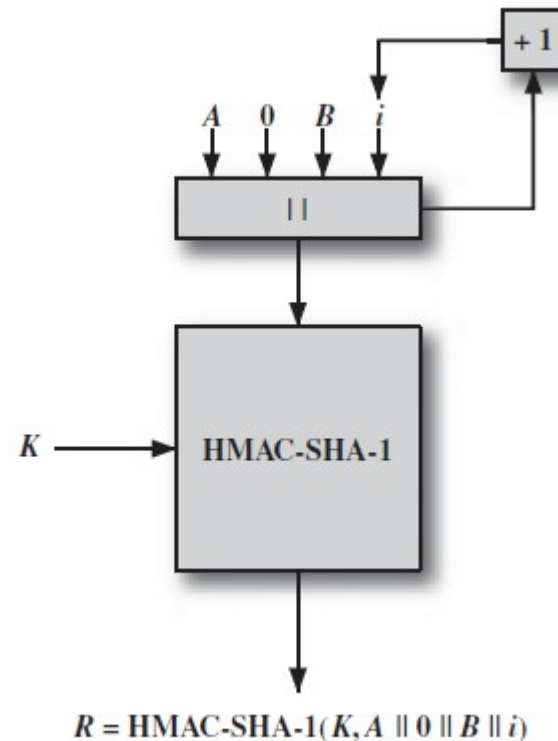


Figure 6.10 IEEE 802.11i Pseudorandom Function