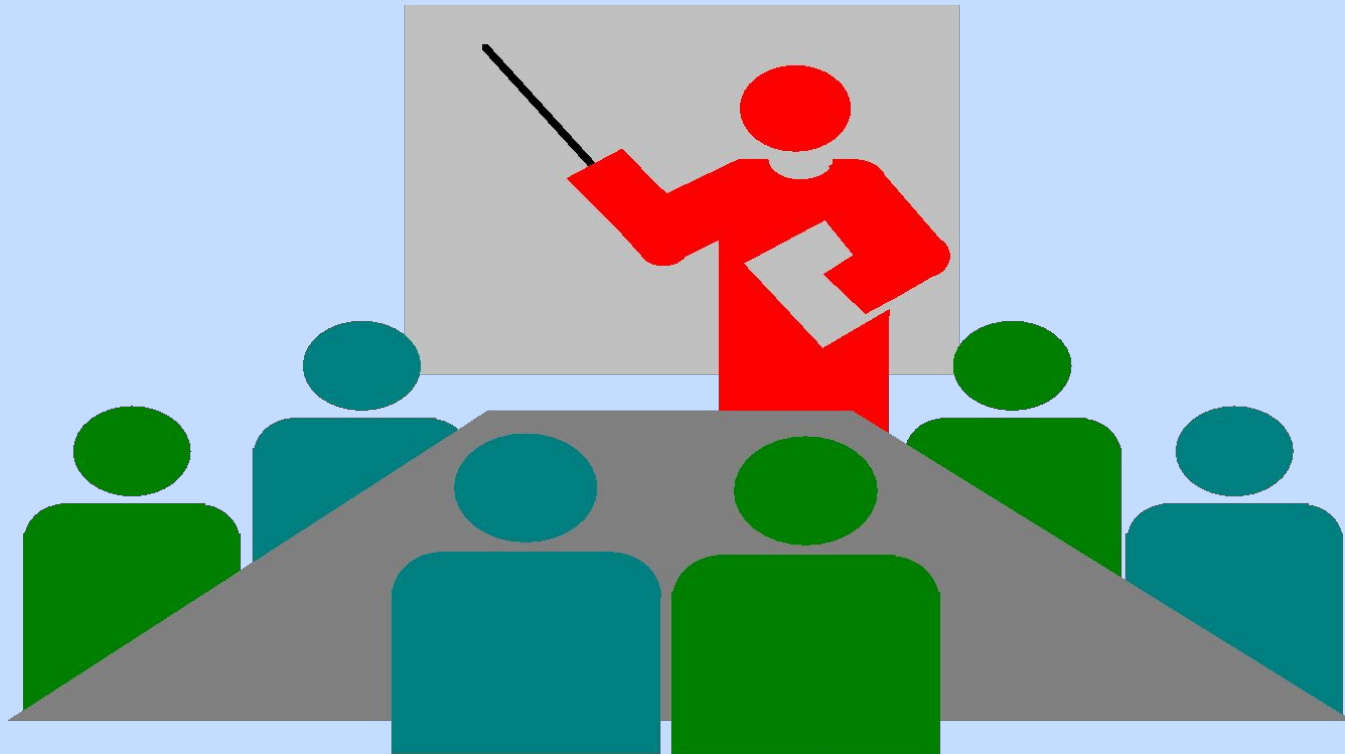


Wireless Network Security

Dr.Eng.Bader Ahmad



IEEE 802.11

- IEEE 802 committee for LAN standards
- IEEE 802.11 formed in 1990's
charter to develop a protocol & transmission specifications for wireless LANs (WLANs)
- since then demand for WLANs, at different frequencies and data rates, has exploded
- hence seen ever-expanding list of standards issued

IEEE 802 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

IEEE 802 Terminology

- **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) :**

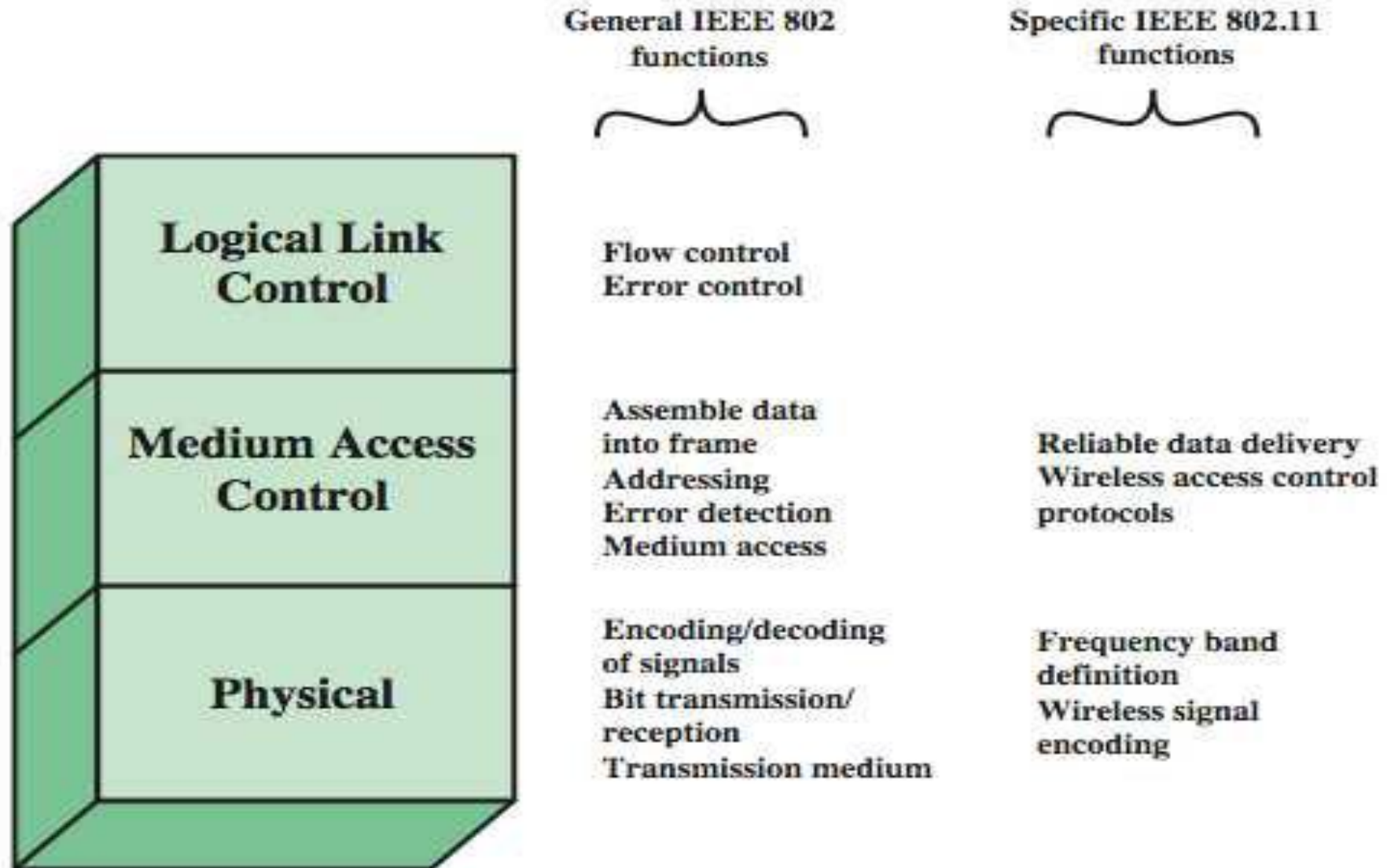
Information that is delivered as a unit between MAC Users .

- **Station :** Any device that contains an IEEE 802.11 conformant MAC and physical layer

Wi-Fi Alliance

- 802.11b first broadly accepted standard
- Wireless Ethernet Compatibility Alliance
- (WECA) industry consortium formed 1999
 - to assist interoperability of products
 - renamed Wi-Fi (Wireless Fidelity) Alliance
 - created a test suite to certify interoperability
 - initially for 802.11b, later extended to 802.11g
 - concerned with a range of WLANs markets, including enterprise, home, and hot spots

IEEE 802 Protocol Architecture



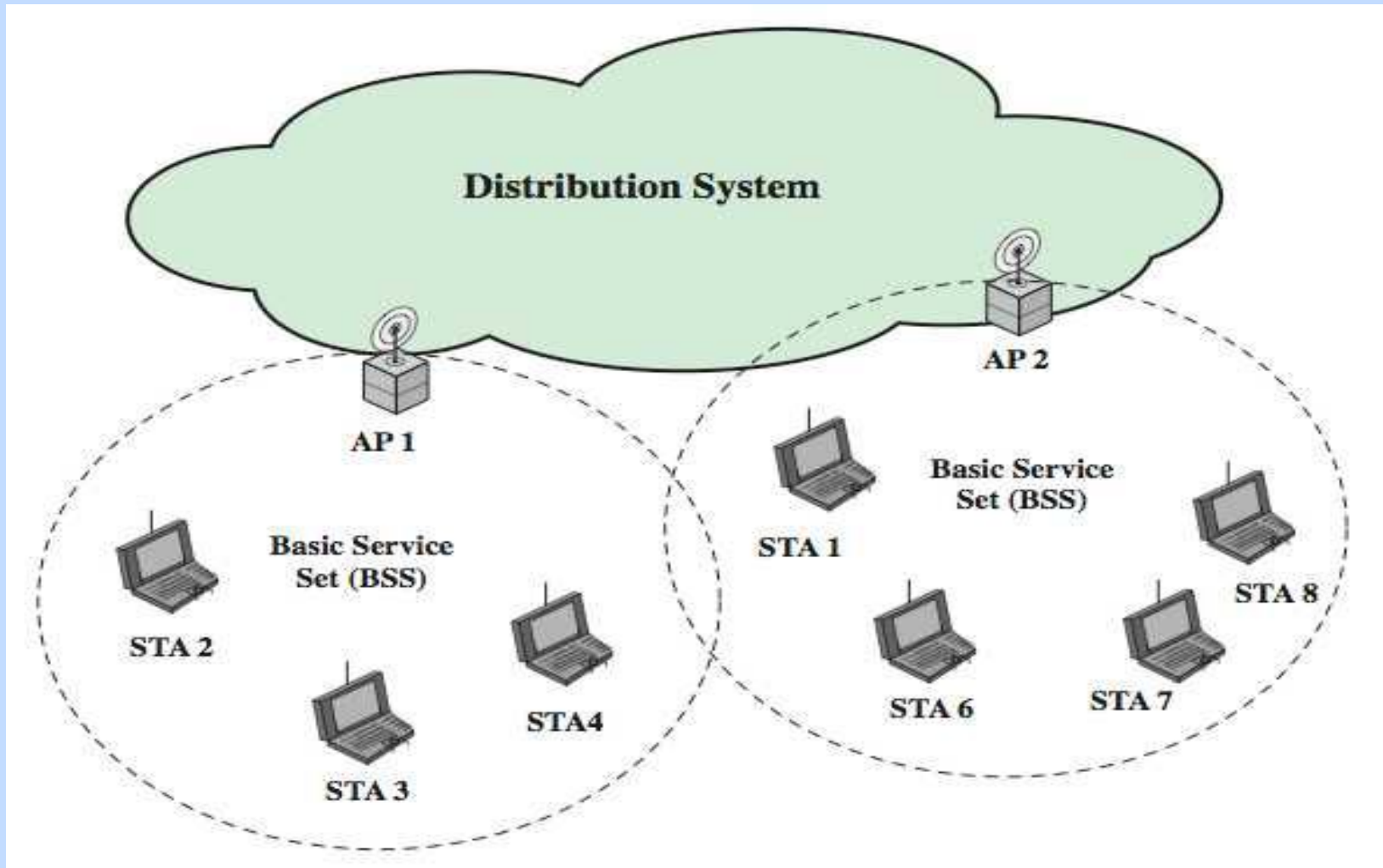
IEEE 802 Protocol Architecture

- **IEEE 802 physical layer includes:**
 - • Encoding/decoding of signals
 - • Transmission/reception
 - • Specification of the transmission medium.
- • **IEEE 802.11 physical layer also defines:**
 - • Frequency bands
 - • Antenna characteristics.

IEEE 802 Protocol Architecture

- **Media Access Control (MAC) layer controls access to the transmission medium:**
 - Receives data from a higher-layer protocol (LLC) layer, in the form of a block of data known as **MAC service data unit (MSDU)**
 - Responsible for detecting errors and discarding any frames that contain errors.
- **The Logical Link Control (LLC) layer**
- (optionally) keeps track of which frames have been successfully received and retransmits unsuccessful frames.

Network Components & Architecture



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 Services (9 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 may be implemented in an AP or in another special-purpose device attached to the distribution system.

IEEE 802.11 Services (9 Services)

- Three services control IEEE 802.11 LAN access and confidentiality:
 - –Authentication, Deauthentication and Privacy
- Six services 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.
 - –Association, Reassociation, Disassociation, Distribution, Integration and MSDU delivery

IEEE 802.11 Services (9 Services)

- **MSDU delivery**, basic service, in which the information that is delivered as a unit between MAC users.
- **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.
- **Integration**, enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated (wired) IEEE 802.x LAN. To deliver a message within a DS, the distribution service needs to know where the destination station is located.

IEEE 802.11 Services (9 Services)

- **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.

802.11 Wireless LAN Security

- wireless traffic can be monitored by any radio in range, not physically connected
- original 802.11 spec had security features
 - **Wired Equivalent Privacy (WEP) algorithm**
 - But found this contained major weaknesses
- 802.11i task group developed capabilities to address WLAN security issues
 - Wi-Fi Alliance **Wi-Fi Protected Access (WPA)**
 - final 802.11i **Robust Security Network (RSN)**

802.11i RSN Services and Protocols

Robust Security Network (RSN)

Services

Access Control

Authentication
and Key
Generation

Confidentiality, Data
Origin Authentication
and Integrity and
Replay Protection

Protocols

IEEE 802.1
Port-based
Access Control

Extensible
Authentication
Protocol (EAP)

TKIP

CCMP

802.11i RSN Services and Protocols

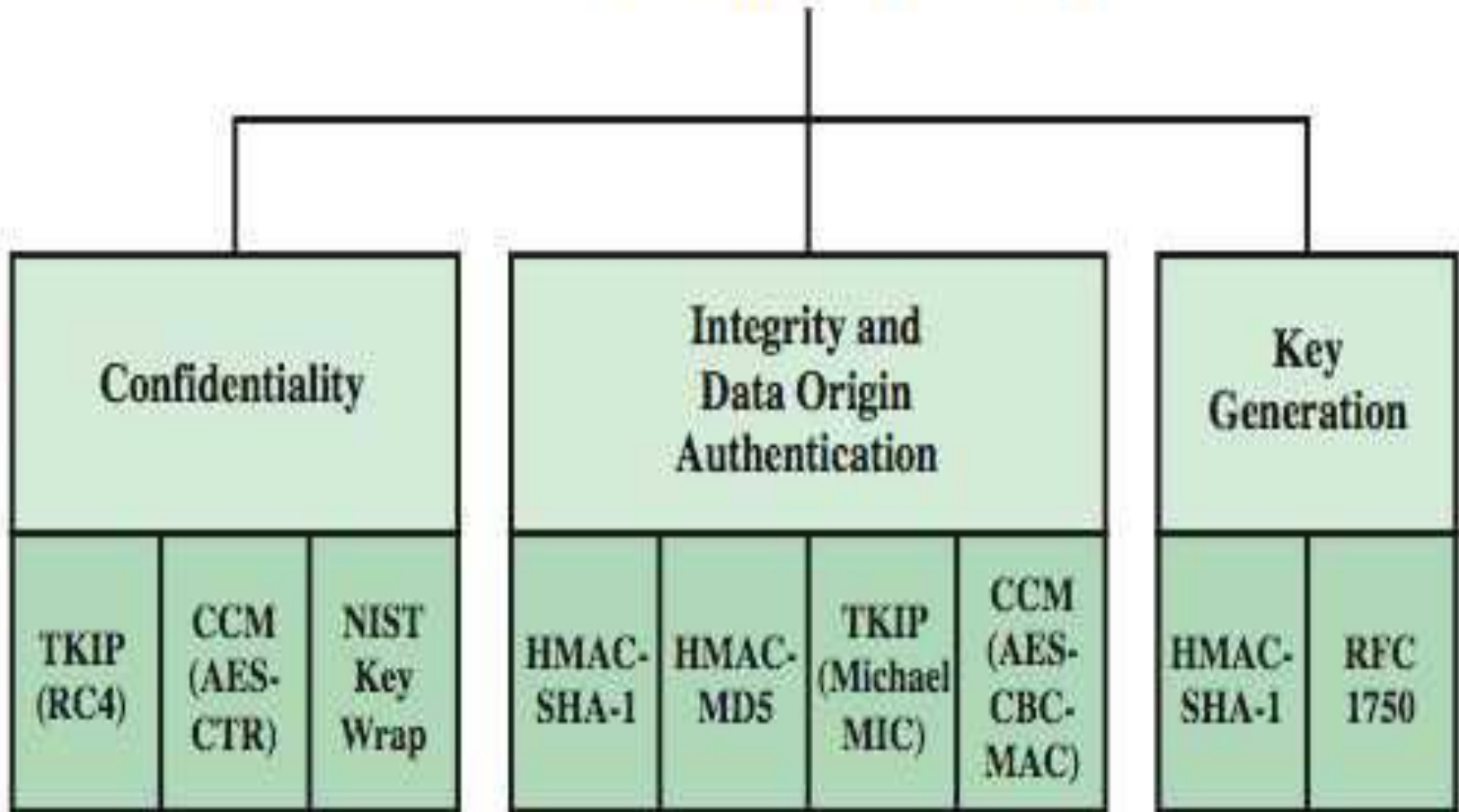
- The 802.11i RSN security specification defines the following services:
 - **Authentication**: A protocol is used to define an exchange between a user and AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
 - **Access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

802.11i RSN Cryptographic Algorithms

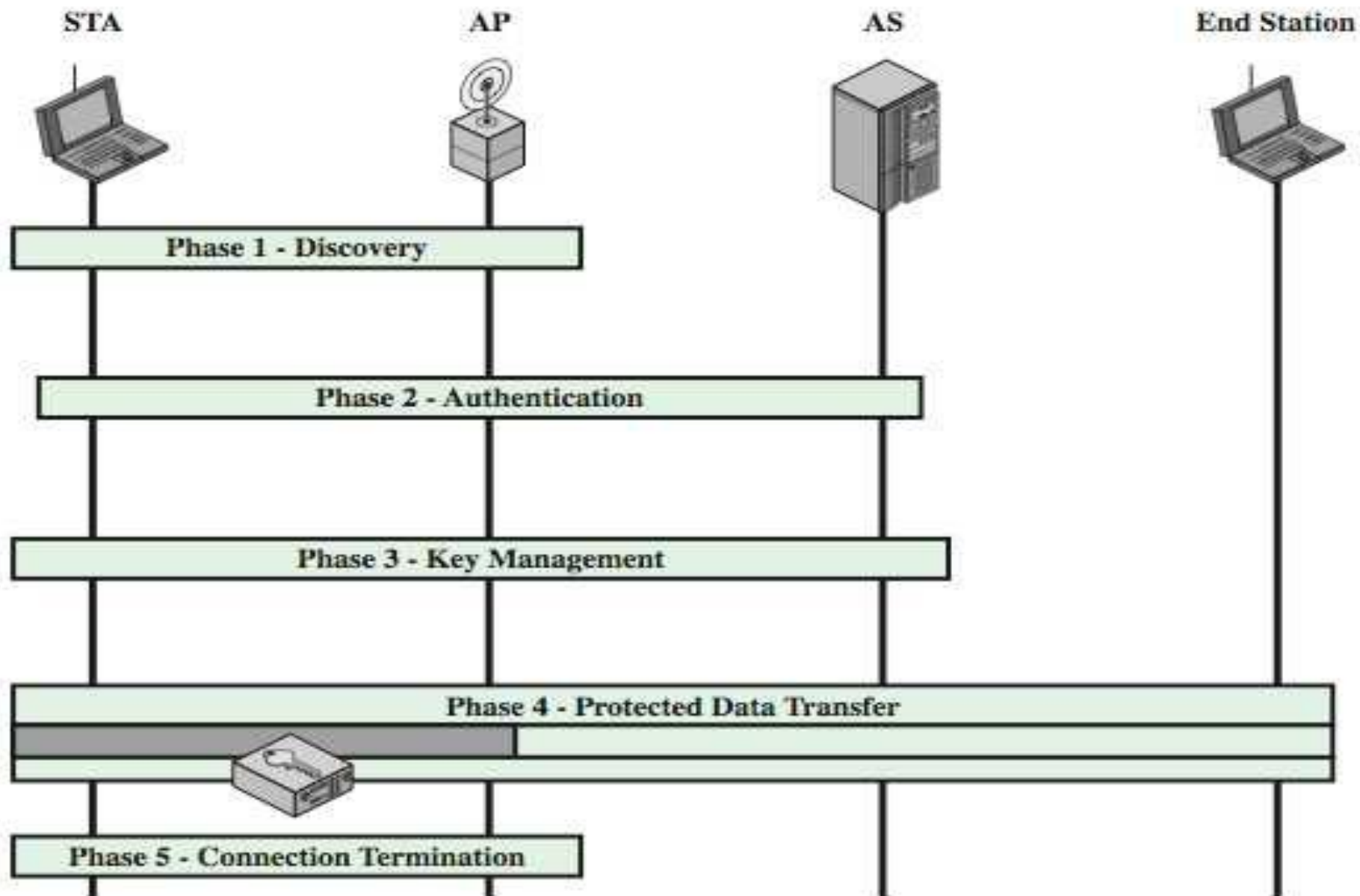
Robust Security Network (RSN)

Services

Algorithms



802.11i Phases of Operation



802.11i Phases of Operation

- IEEE 802.11i RSN operation can be broken down into five distinct phases of operation
- • **Discovery:** AP uses messages called Beacons and Probe Responses to advertise its IEEE802.11i security policy. STA uses these to identify AP for a WLAN with which it wishes to communicate. STA associates AP, which it uses to select the cipher suite and authentication mechanism when Beacons and Probe Responses present a choice.
- • **Authentication:** STA and AS prove their identities to each other. AP blocks non-authentication traffic between STA and AS until the authentication transaction is successful. AP does not participate in the authentication transaction other than forwarding traffic between STA & AS.

802.11i Phases of Operation

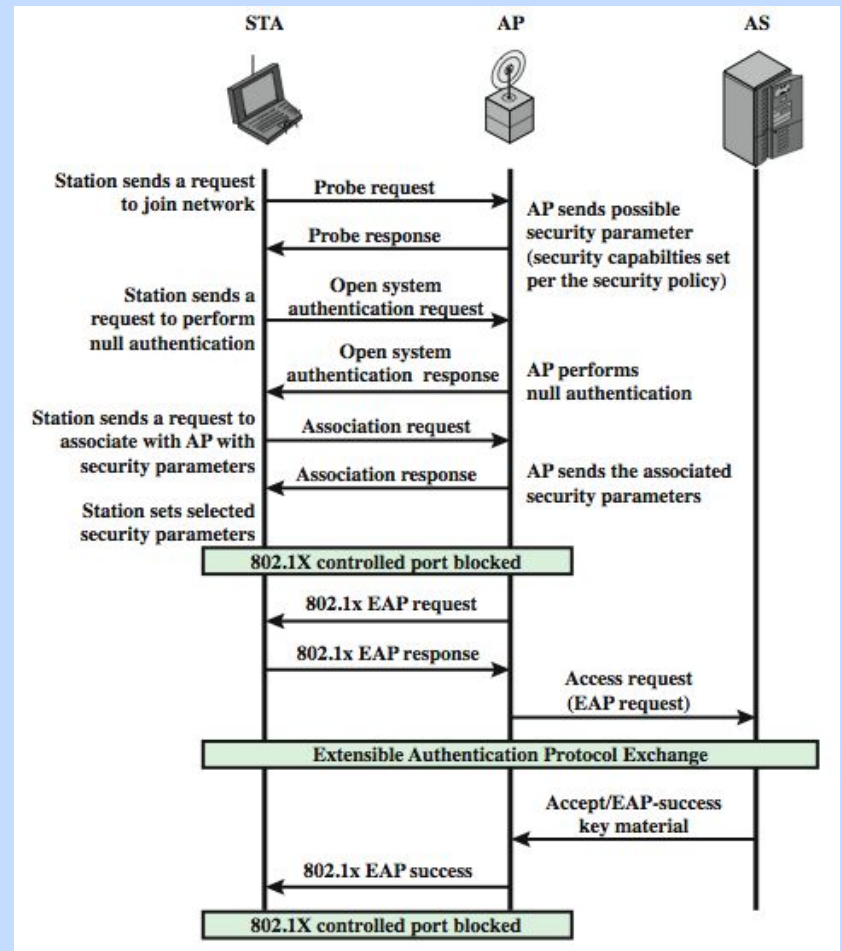
- • **Key generation and distribution:** AP and STA perform several operations that cause cryptographic keys to be generated and placed on AP and STA. Frames are exchanged between AP and STA only
- • **Protected data transfer:** Frames are exchanged between STA and end station through AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between STA and AP only; security is not provided end-to-end.
- • **Connection termination:** AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.

802.11i

Discovery and Authentication Phases

The Discovery phase is for an STA and an AP to recognize each other, agree on a set of security capabilities, and establish an association for future communication.

It consists of three exchanges: Network and security capability discovery, Open system authentication, and Association.

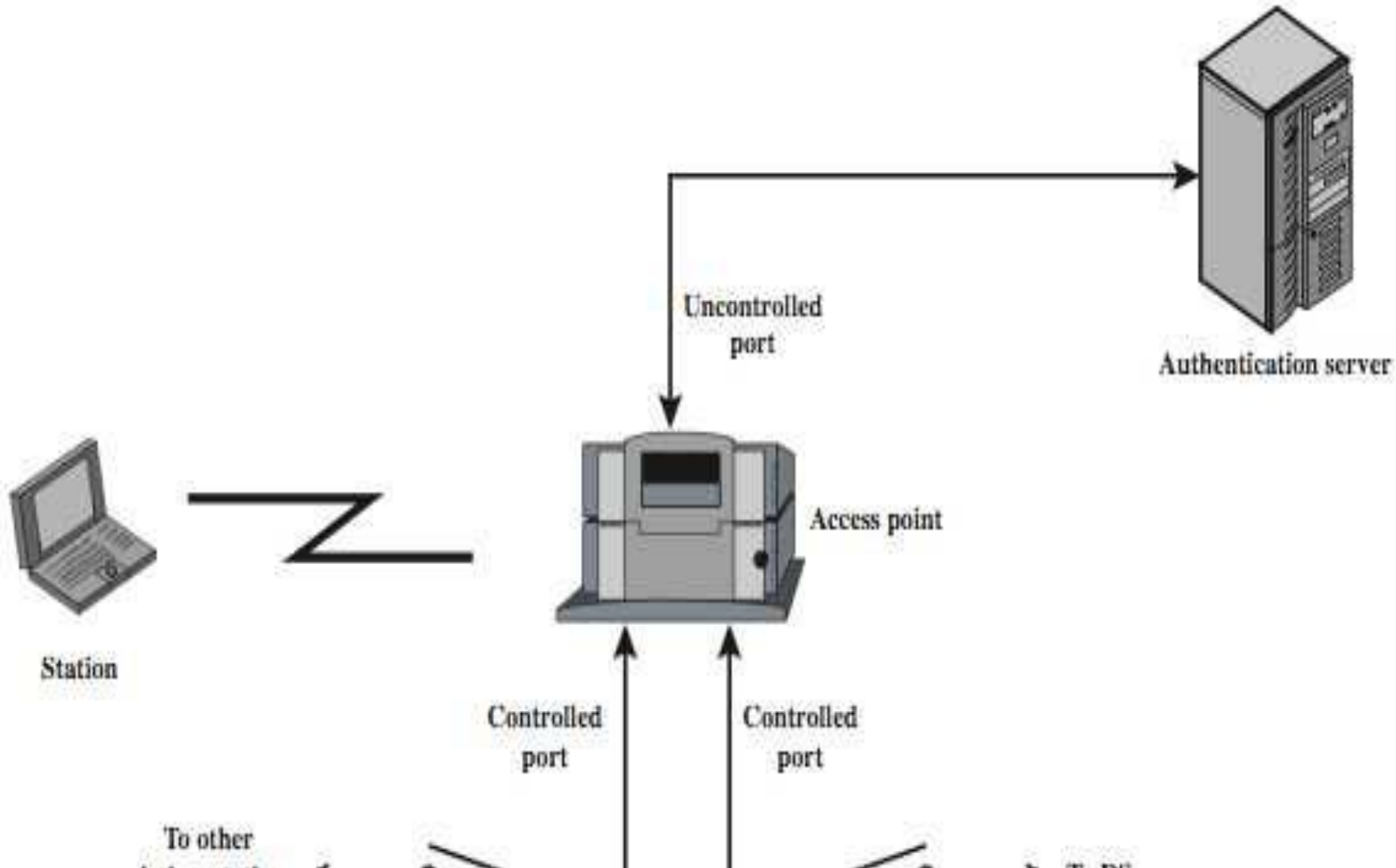


802.11i

Discovery and Authentication Phases

- **The authentication phase** enables mutual authentication between an STA and an authentication server (AS) located in the DS. **Authentication** is designed to allow only authorized stations to use the network and to provide the STA with assurance that it is communicating with a legitimate network

IEEE 802.1X Access Control Approach

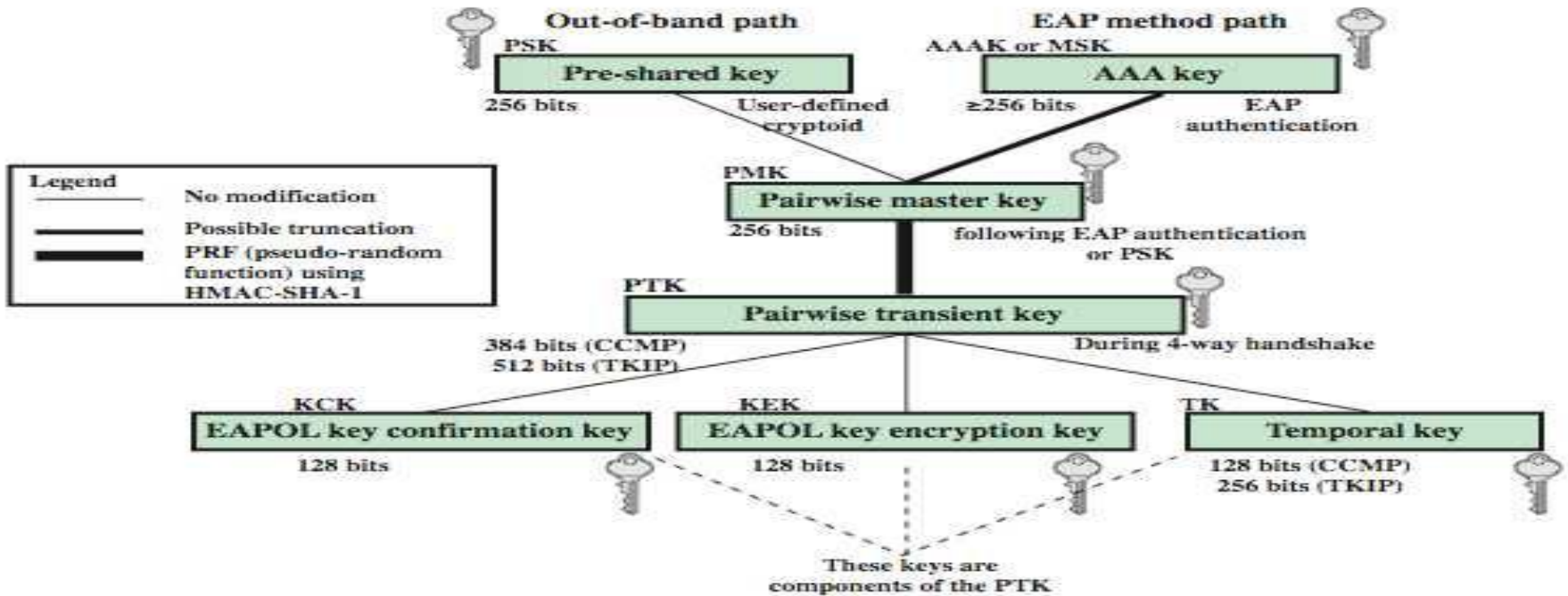


IEEE 802.1X Access Control Approach

- IEEE 802.11i uses the Extensible Authentication Protocol (EAP). Before wireless station (STA) is authenticated by AS, the (AP) only passes control or authentication messages between STA and AS.
- The 802.1X control channel is unblocked but the 802.11 data channel is blocked.
- Once STA is authenticated and keys are provided, the AS can forward data from STA, subject to predefined access control limitations for STA to the network and the data channel is unblocked

802.11i

Key Management Phase



(a) Pairwise key hierarchy



(b) Group key hierarchy

802.11i

Key Management Phase

- 802.11i Key Management Phase
- • AP controlled ports remain blocked until the temporal keys are installed in the STA and AP, which occurs during the 4-Way Handshake.
- • A variety of cryptographic keys are generated and distributed to STAs.
- • There are two types of keys:
- • **Pairwise keys**, used for communication between STA and AP;
- • **Group keys**, for multicast communication.
- • **Pairwise keys** form a hierarchy, beginning with a master key from which other keys are derived dynamically and used for a limited period of time.

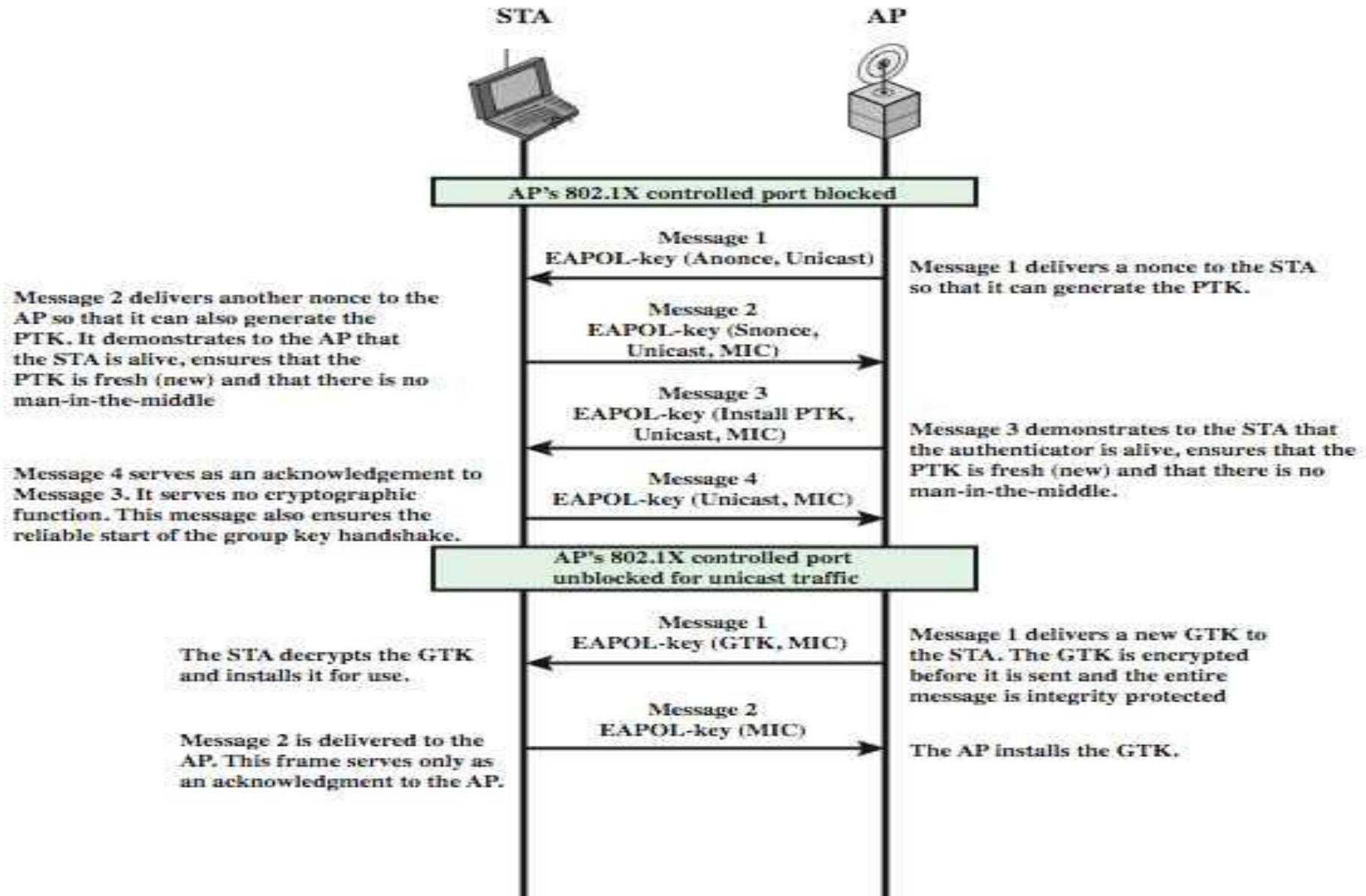
802.11i

Key Management Phase

- • **Pre-shared key (PSK)** A secret key shared by AP and STA
- • **Master session key (MSK)**, which is generated using the IEEE 802.1X protocol during the authentication phase,
- • **Pairwise master key (PMK)** is derived from the master key as follows:
 - • If PSK is used, then PSK is used as the PMK;
 - • If MSK is used, then PMK is derived from MSK. By the end of the authentication phase both AP and STA have a copy of their shared PMK.
- • PMK is used to generate **pairwise transient key (PTK)**, which in fact consists of three keys to be used for communication between an STA and AP after they have mutually authenticated.

802.11i

Key Management Phase



802.11i

Key Management Phase

- **4-way handshake exchange MPDU for distributing pairwise keys. STA and AP confirm the existence of the PMK, verify the selection of the cipher suite, and derive a fresh PTK for the following data session.**
- **For group key distribution, the AP generates a GTK and distributes it to each STA in a multicast group.**

802.11i

Protected Data Transfer Phase

- have two schemes for protecting data
- **Temporal Key Integrity Protocol (TKIP)**
 - changes only to older WEP
 - adds 64-bit Michael message integrity code
- (MIC)
- encrypts MPDU plus MIC value using RC4
- **Counter Mode-CBC MAC Protocol (CCMP)**
 - uses the cipher block chaining message
 - authentication code (CBC-MAC) for integrity
 - uses the CRT block cipher mode of operation

Wireless Application Protocol (WAP)

- •(WAP) is a universal, open standard developed by the WAP Forum to provide mobile users of wireless phones and other wireless devices, access to telephony and information services.
- •WAP is designed to work with all wireless network technologies (e.g., GSM, CDMA, TDMA).
- •WAP is based on existing Internet standards, such as IP, XML, HTML, and HTTP, as much as possible, & also includes security facilities.
- •Strongly affecting the use of mobile phones and terminals for data services are the significant limitations of the devices (in processors, memory, and battery life) and the networks (relatively low bandwidth, high latency, and unpredictable availability and stability) that connect them.

Wireless Application Protocol (WAP)

- • WAP specification includes:
 - • A programming model based on the WWW Programming Model
 - • A markup language, the Wireless Markup Language, adhering to XML
 - • A specification of a small browser suitable for a mobile, wireless terminal
 - • A framework for wireless telephony applications (WTAs)

WAP Infrastructure

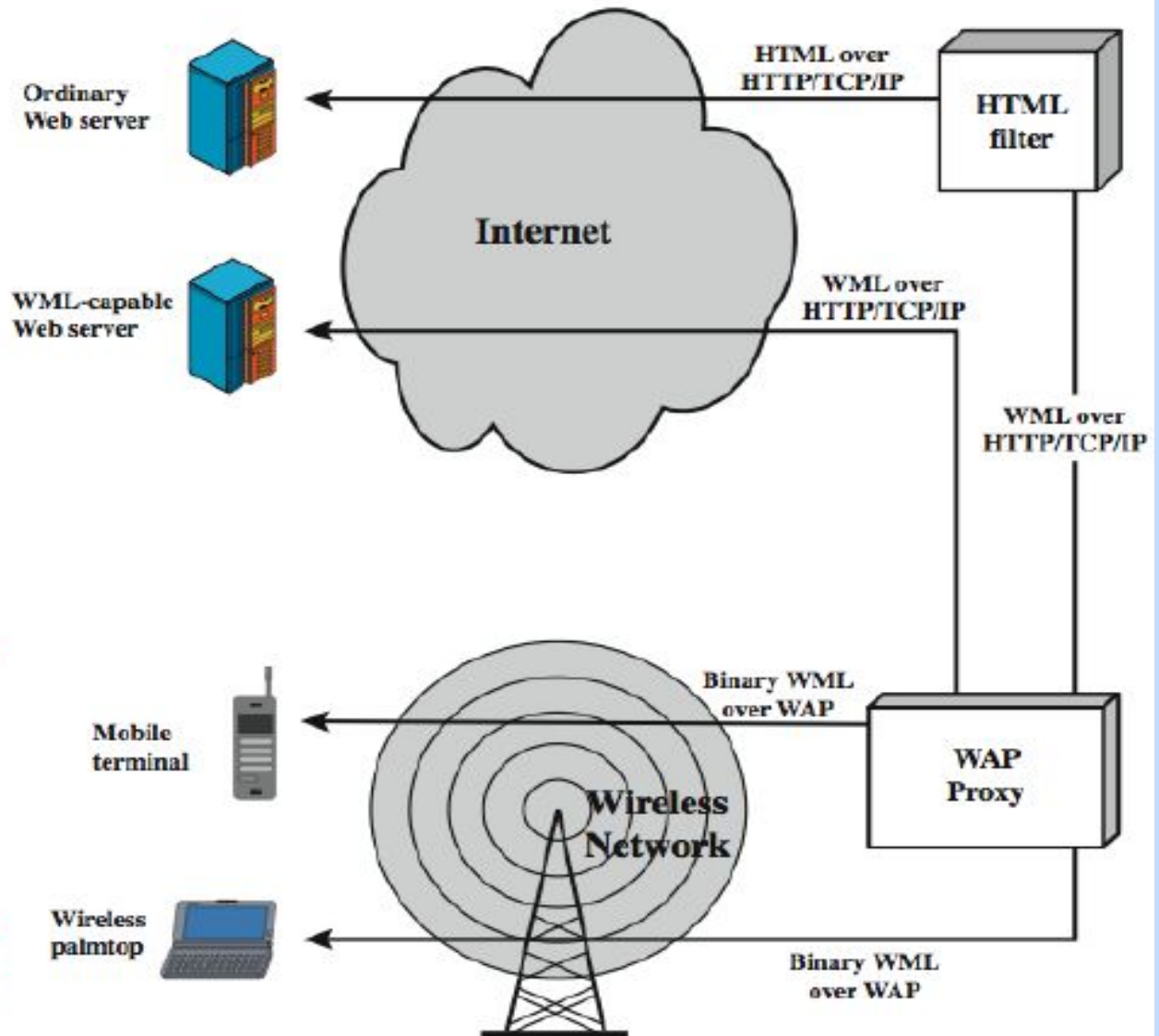
WAP Infrastructure

* HTML content must go through an HTML filter.

* The filter translates the HTML content into WML content.

* The proxy converts the WML into binary WML and delivers it to the mobile user over a wireless network using the WAP protocol stack.

* If the Web server is capable of directly generating WML content, then the WML is delivered using HTTP/TCP/IP to the proxy.



Summary

- have considered:
 - IEEE 802.11 Wireless LANs
 - protocol overview and security
 - Wireless Application Protocol (WAP)
 - protocol overview

بعض الاختصارات

- WECA : Wireless Ethernet Compatibility Alliance
- MAC : Media Access Control Layer
- LLC : Logical Link Control
- IBSS : independent BSS
- WEP : Wired Equivalent Privacy
- WPA : Wi-Fi Protected Access
- RSN : Robust Security Network
- EAP : Extensible Authentication Protocol
- TKIP : Temporal Key Integrity Protocol
- CCMP : Counter Mode with Cipher Block Chaining MAC Protocol
- CCM : Counter Mode with Cipher Block Chaining Message Authentication Code
- CBC-MAC : Cipher Block Block Chaining Message Authentication Code
- PSK : A pre-shared key
- MSK : master session key
- PMK : pairwise master key
- MIC : message integrity code PRF