Unit: Network Security

B.Tech VIII

NETWORK AND SYSTEM SECURITY (CORE ELECTIVE - 5) (CS424)

Book :

Computer Security: Principles and Practice
By William Stallings

Chapter 22: Internet Security Protocols and Standards
Chapter 23: Internet Authentication Applications
Chapter 24: Wireless Network Security

Contents

- **Chapter 24: Wireless Network Security**
  - Wireless Security
  - IEEE 802.11 Wireless LAN Overview
  - IEEE 802.11i Wireless LAN Security
  - Network Management Security-SNMP Protocol

Wireless Security

Wireless Security: Overview

- A **wireless network** is a computer network that uses wireless data connections between network nodes.
- It is **cost effective** as it enables communication without the use of costly cable connection between distant equipment.
- **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 Security: Overview

- Key factors contributing to the higher security risk of wireless networks compared to wired networks are
- **Channel:**
  - Wireless networking 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:**
  - Usually, the wireless devices are more portable and mobile than wired devices. Such mobility results in variety of risks.

Wireless Security: Overview

- Key factors contributing to the higher security risk of wireless networks compared to wired networks are
- **Resources::**
  - Some wireless devices, such as smartphones and tablets, have sophisticated OS but limited memory and processing resources with which to counter threats, including denial of service and malware is difficult.
- **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 Security: Overview

- The wireless environment consists of three components that provide point of attack.

1. **Wireless client (Endpoint)**: a cell phone, a Wi-Fi enabled laptop or tablet, a wireless sensor, a Bluetooth device, and so on.
2. **Wireless Access point:** provides a connection to the network. example of access points are cell towers, Wi-Fi hot spots, and wireless access points to wired local or wide-area networks.
3. **Transmission medium:** which carries the radio waves for data transfer, is also a source of vulnerability.

Figure 24.1 **Wireless Networking Components**

Wireless Network Threats

- **Accidental association:**
  - Overlapping of frequency ranges
  - Two wireless LANs residing in close proximity (e.g., in the same or neighbouring buildings) may create overlapping transmission ranges.
  - A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighbouring 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.

Wireless Network Threats

- **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.
- **Non-traditional networks:**
  - Non-traditional networks and links, such as personal network Bluetooth devices, barcode readers, and handheld PDAs pose a security risk both in terms of 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.

Wireless Network Threats

- **Man-in-the middle attacks:**
  - It 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):**
  - It occurs when an attacker continually sends messages to a wireless access point or some other accessible wireless port with various protocol 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.

Wireless Security Measures

- Wireless security measures are grouped according to the elements of wireless communication network
  1. Security measures for wireless transmissions,
  2. Security measures for wireless access points,
  3. Security measures for wireless networks (consisting of wireless routers and endpoints).

Wireless Security Measures

1. 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.

1. Signal-hiding techniques:

- Includes number of measures to make it more difficult for an attacker to locate their wireless access points.
- turning off service set identifier (SSID) broadcasting by wireless access points, - assigning cryptic names to SSIDs - reducing signal strength to the lowest level that still provides requisite coverage - locating wireless access points in the interior of the building etc.

2. Encryption:

- Encryption of all wireless transmission is effective against eavesdropping to the extent that the encryption keys are secured.

Wireless Security Measures

2. 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(fake) access points and other unauthorized devices from becoming insecure backdoors.

Wireless Security Measures

3. **Securing Wireless Network**
    1. **Use encryption:** Wireless routers are typically equipped with built-in encryption mechanisms for router-to-router traffic.
    2. **Use anti-virus and anti-spyware software, and a firewall:** These facilities should be enabled on all wireless network endpoints.
    3. **Turn off identifier broadcasting:** Wireless routers are typically configured to broadcast an identifying signal so that any device within range can learn of the router's existence. If a network is configured so that authorized devices know the identity of routers, this capability can be disabled, so as to thwart attackers.
    4. **Change the identifier on router from the default:** this measure thwarts attackers who will attempt to gain access to a wireless network using default router identifiers.

Wireless Security Measures

3. **Securing Wireless Network(Cont..)**
   5. **Change router's pre-set password for administration:** This is another prudent step.
   6. **Allow only specific computers to access your wireless network:** A router can be configured to only communicate with approved MAC addresses.

IEEE 802.11 Wireless LAN

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).
- The first 802.11 standard to gain broad industry acceptance was **802.11b**.
- In 1999, the **Wireless Ethernet Compatibility Alliance (WECA),** an industry consortium, was formed to meet the requirement that the wireless products designed based on the same standard 802.11 should interoperate even though they came from different vendors.
- WECA 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.***

IEEE 802.11 Wireless LAN : Overview

- 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 Protocol Architecture

- **IEEE 802.11** standards are defined within the structure of a layered set of protocols.

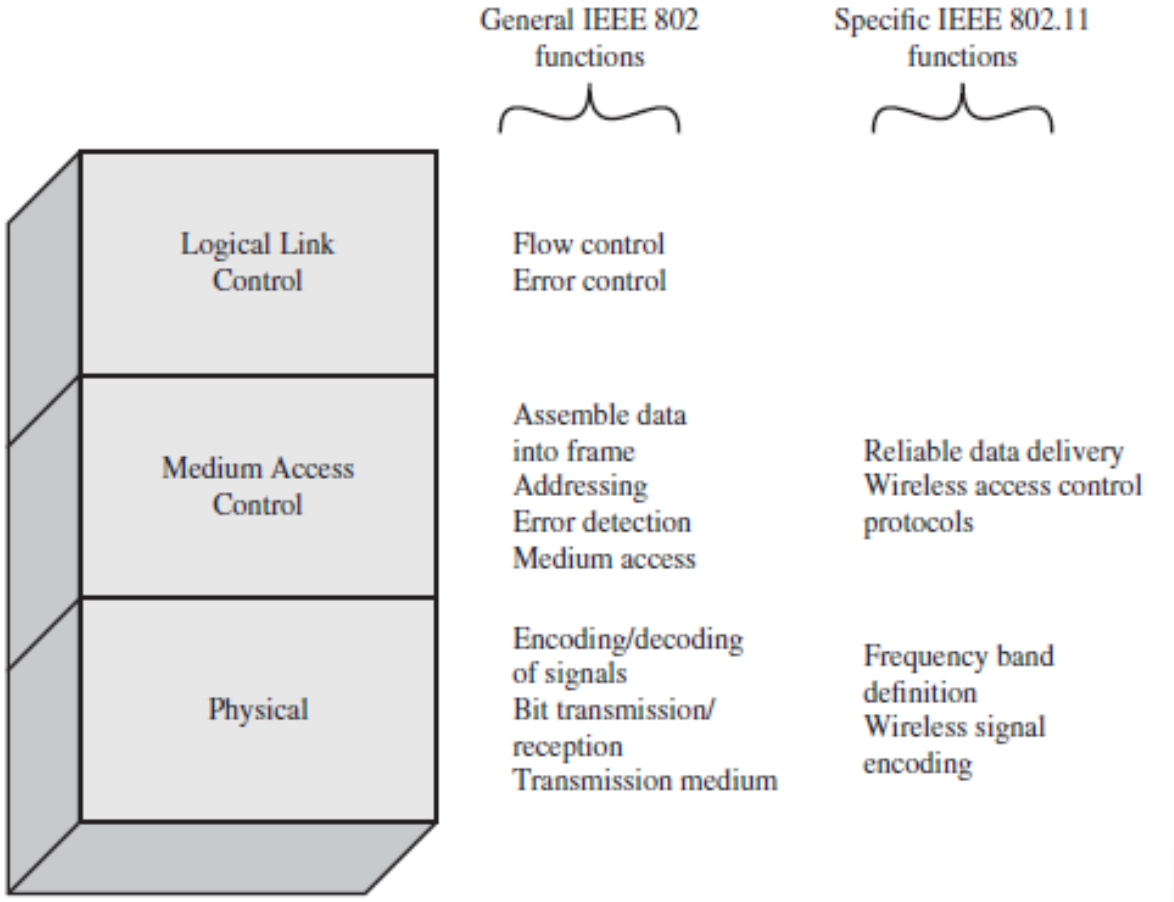


Figure 24.3 **IEEE 802.11 Protocol Stack**

IEEE 802 Protocol Architecture

- **IEEE 802.11** standards are defined within the structure of a layered set of protocols.
- **Physical Layer**
  - The lowest layer of the IEEE 802 reference model is the **physical layer**, which includes such functions as encoding/decoding of signals and bit transmission/reception.
  - It also includes a specification for frequency bands and antenna characteristics.

IEEE 802 Protocol Architecture

- **IEEE 802.11** standards are defined within the structure of a layered set of protocols.
- **Medium Access Control Layer**
  - 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 known as the MAC service data unit (MSDU).**
  - In general, the MAC layer performs the following functions:

1. On transmission, assemble data into a **frame**, known as a **MAC Protocol Data Unit (MPDU) with address and error-detection fields.**
2. On reception, disassemble frame, and perform address recognition and error detection.
3. Govern access to the LAN transmission medium.

IEEE 802 Protocol Architecture

- **IEEE 802.11** standards are defined within the structure of a layered set of protocols.
- **Medium Access Control Layer (cont..)**
  - **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.

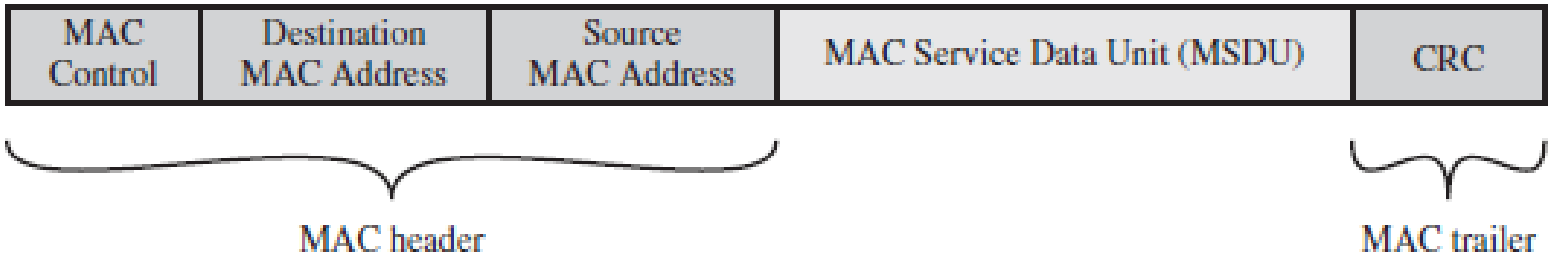


Figure 24.4 **General IEEE 802 MPDU Format**

IEEE 802 Protocol Architecture

- **IEEE 802.11** standards are defined within the structure of a layered set of protocols.
- **Medium Access Control Layer (cont..)**
  - **MAC Service Data Unit:** The data from the higher layer.
  - **CRC:** The **cyclic redundancy check** field, also known as the **Frame Check Sequence (FCS)** field. This is an error-detecting code. 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 do not match, then one or more bits have been altered in transit.

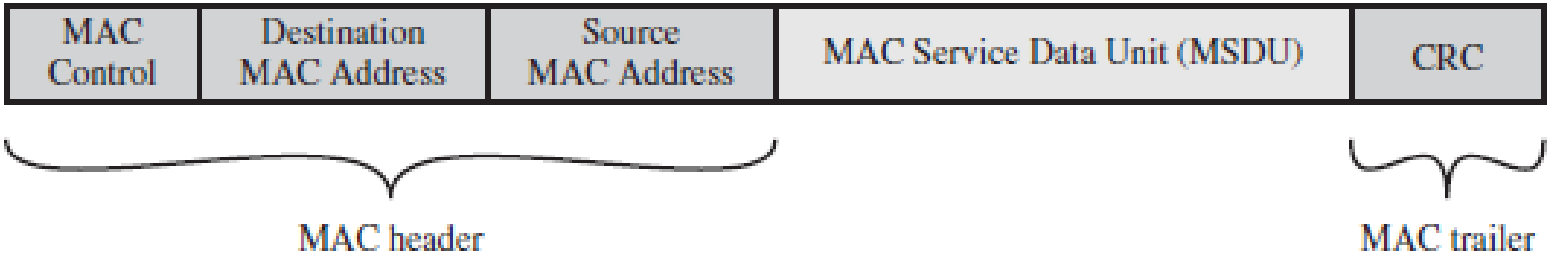


Figure 24.4 **General IEEE 802 MPDU Format**

IEEE 802 Protocol Architecture

- **IEEE 802.11** standards are defined within the structure of a layered set of protocols.
- **Logical Link Control Layer**
  - The LLC layer optionally keeps track of which frames have been successfully received and retransmits unsuccessful frames.

IEEE 802.11 Network Components and Architectural Model

Table 24.1 **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 802.11 Network Components and Architectural Model

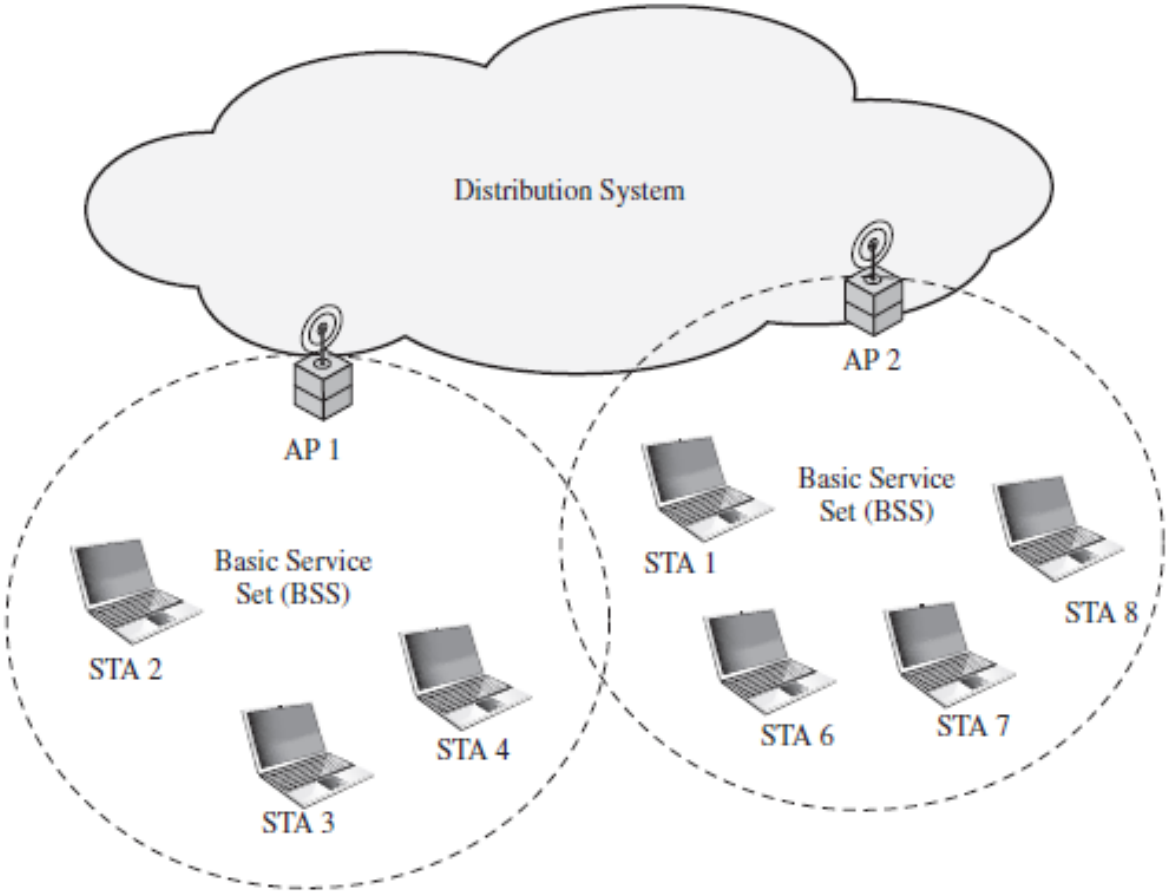


Figure 24.5 **IEEE 802.11 Extended Service Set**

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 executing the same MAC protocol and competing for access to the same shared wireless medium.
- 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 a BSS, client stations do not communicate directly with one another.
- 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.
- Similarly, a MAC frame from a station in the BSS to a remote station is sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station.

IEEE 802.11 Network Components and Architectural Model

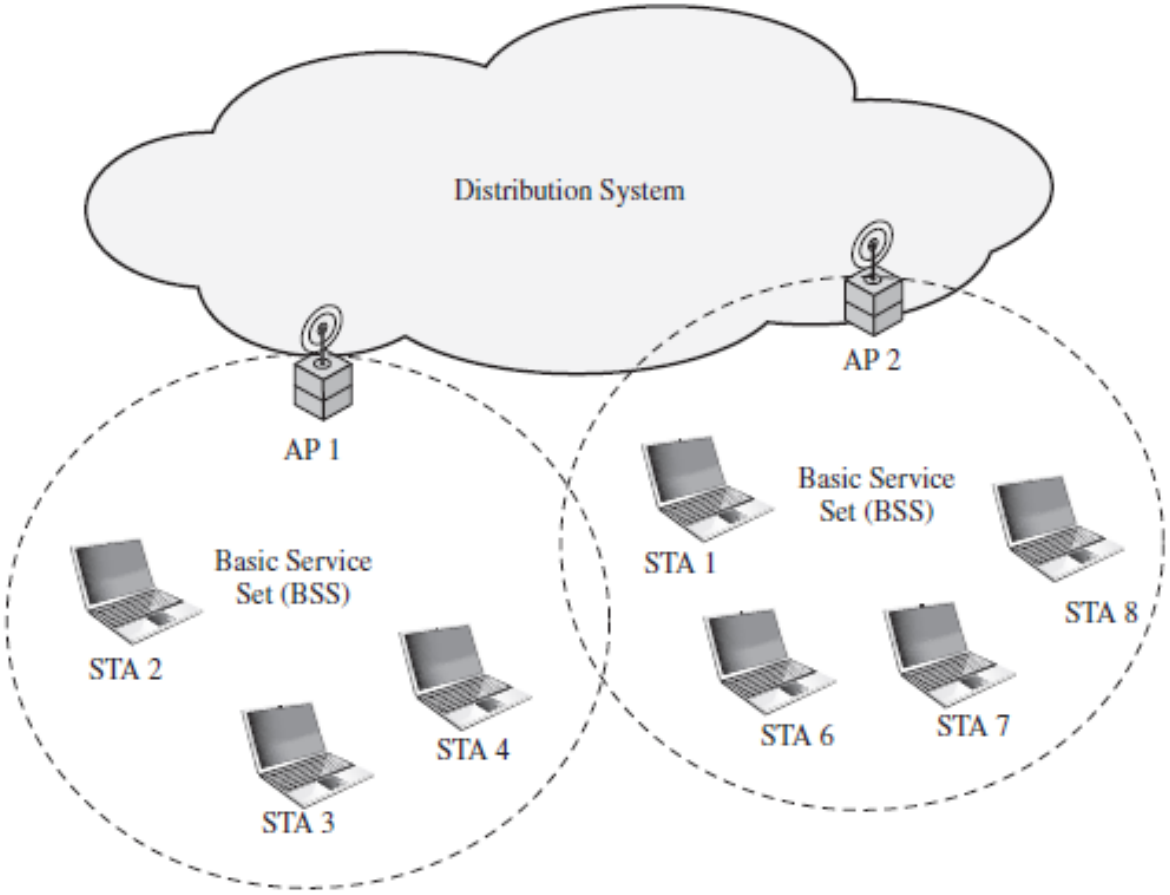


Figure 24.5 **IEEE 802.11 Extended Service Set**

IEEE 802.11 Network Components and Architectural Model

- The BSS generally corresponds to what is referred to as a **cell** in the literature.
- The **DS can be a switch, a wired network, or a wireless network.**
- 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 IBSS is typically an ad hoc network.** In an IBSS, the stations all communicate directly, and no AP is involved.
- An **extended service set (ESS)** consists of two or more BSSs interconnected by a distribution system.
- The extended service set appears as a single logical LAN to the LLC level.

IEEE 802.11 Services

- IEEE 802.11 defines **nine services** and they are listed in **two categories: (i) Service Provider, (ii) Service used to support**

Table 24.2 **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

- **Service provider:**
  - Service provider can be either the station or the Distribution System.
  - **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.

Table 24.2 **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

- **Support:**
  - **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.

Table 24.2 **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:**
- **The two services** involved with the distribution of messages within a DS are **distribution and integration.**

Table 24.2 **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** is 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.
- Example: A frame is to be sent from STA 2 to STA 7.
- The frame is sent STA 2 → AP1→DS→ AP2 → STA7
- 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.

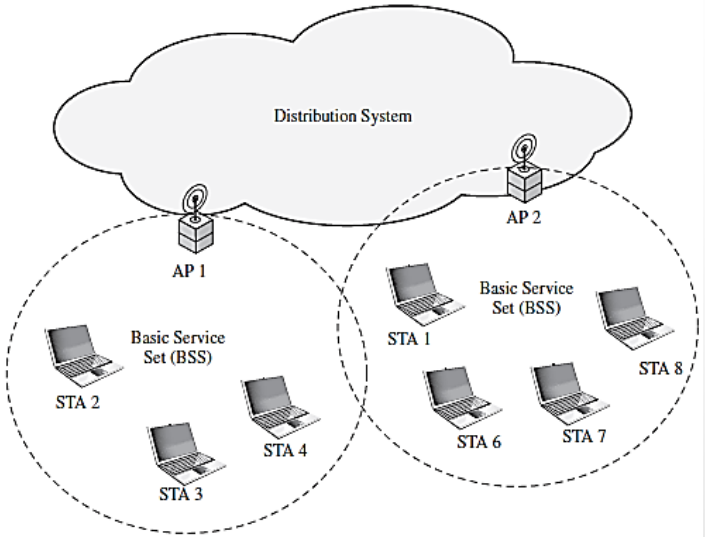


Figure 24.5 IEEE 802.11 Extended Service Set

IEEE 802.11 Services

- **Distribution of Messages Within a DS:**
- The **integration** service enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN.
- The term *integrated* refers to a wired LAN that is physically connected to the DS and whose stations may be logically connected to an IEEE 802.11 LAN via the integration service.
- **The integration service takes care of any address translation and media conversion logic required for the exchange of data.**

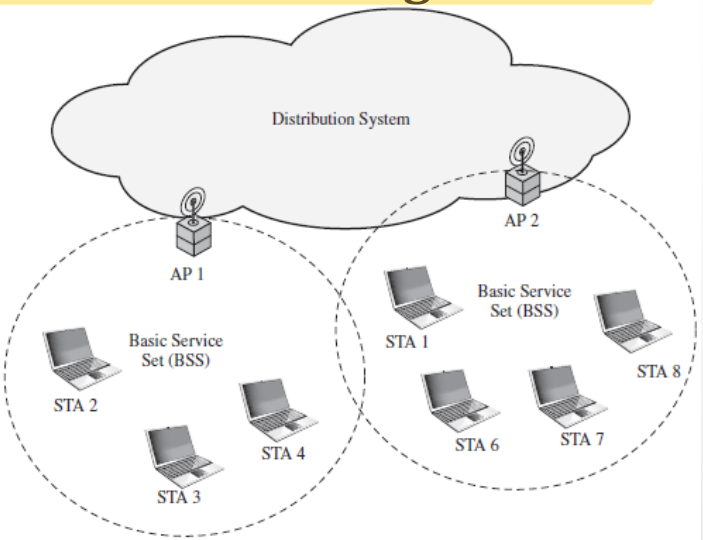


Figure 24.5 IEEE 802.11 Extended Service Set

IEEE 802.11 Services

- **Association-Related Services:**
- The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service.
- For that service to function, it requires **information about stations within the ESS that is provided by the association-related services.**

Table 24.2 **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

- **Association-Related Services (cont..):**
- Before the distribution service can deliver data to or accept data from a station, that station must be *associated*.
- To understand the concepts of association, the concept of mobility (of station) is required.
- There are **three transition types, based on mobility:**
  1. **No transition:** Here, station is either stationary or moves within BSS.
  2. **BSS transition:** Here, station moves from one BSS to another BSS but within same ESS.
  3. **ESS transition:** Here, station moves from one ESS to another ESS.

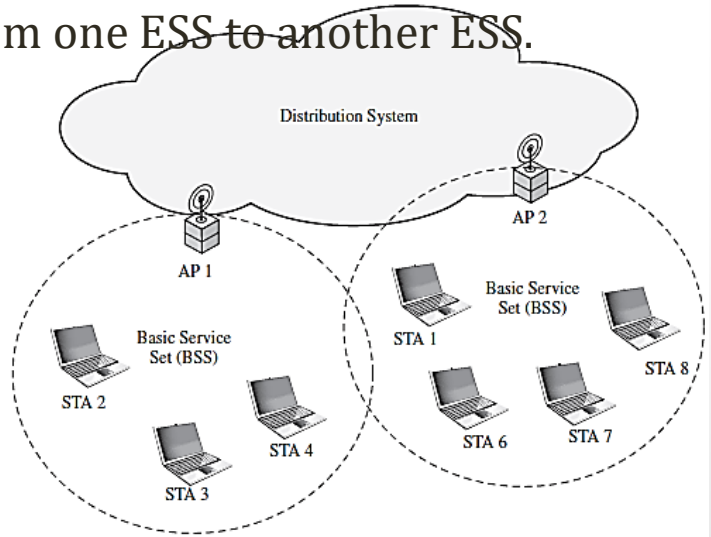


Figure 24.5 IEEE 802.11 Extended Service Set

IEEE 802.11 Services

- **To deliver a message within a DS, the distribution service needs to know where the destination station is located.**
- Specifically, the DS 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.
- To meet this requirement, a station must maintain an association with the AP within its current BSS.
- Three services relate to this requirement:
  - **Association**
  - **Reassociation**
  - **Disassociation:**

Table 24.2 **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

- **Association:**
  - Establishes an initial association between a station and an AP.
  - Before a station can transmit or receive frames on a wireless LAN, its identity and address must be known.
  - For this purpose, a station must establish an association with an AP within a particular BSS.
  - The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.
- **Reassociation:**
  - Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.

IEEE 802.11 Services

- **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.
  - However, the MAC management facility protects itself against stations that disappear without notification.

IEEE 802.11i Wireless LAN

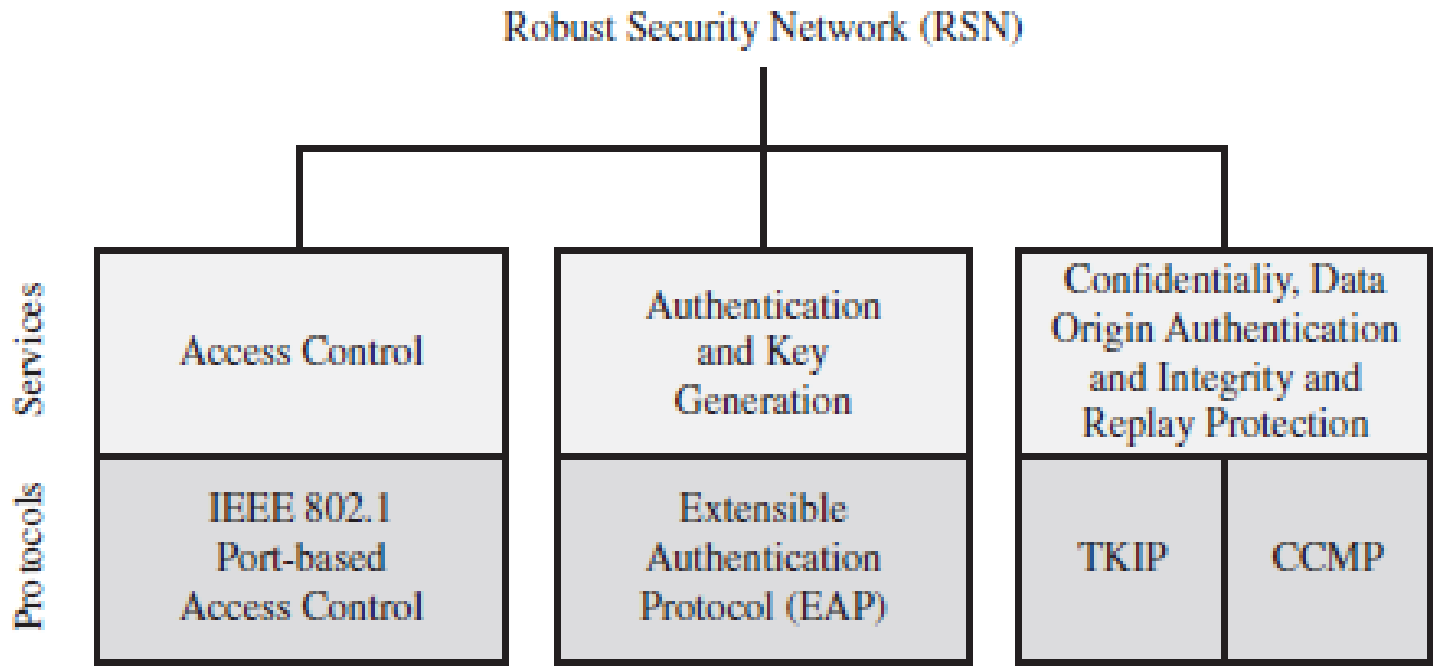
IEEE 802.11i Wireless LAN Security

- The original 802.11 specification included a set of security features for privacy and authentication that were quite weak.
- So the 802.11i task group has developed a set of capabilities to address the WLAN security issues and introduced **Wi-Fi Protected Access (WPA)** as a Wi-Fi standard.
- The final form of the 802.11i standard is referred to as **Robust Security Network (RSN)**.

IEEE 802.11i Services

- **Authentication:**
  - A protocol is used to define an exchange between a user and an AS (authentication server) that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
- **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.

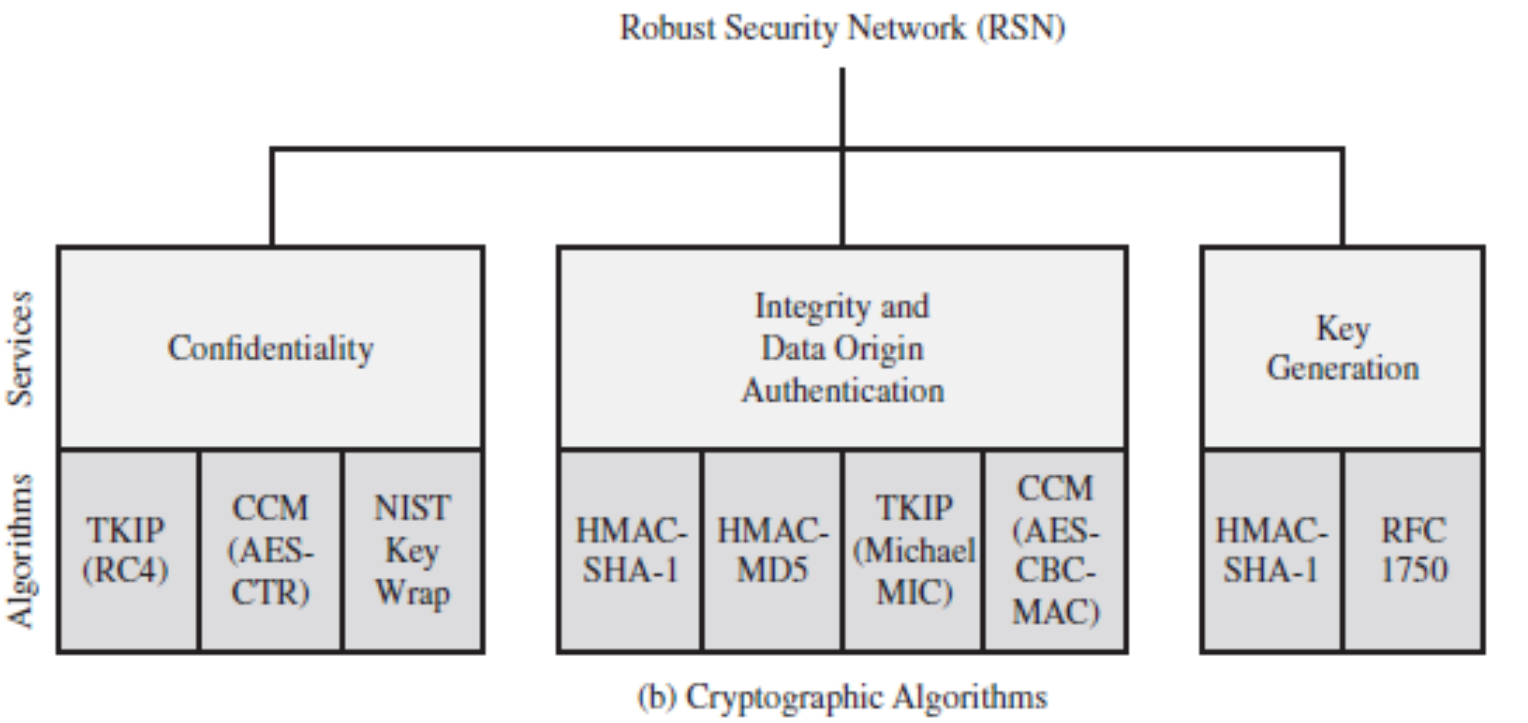
IEEE 802.11i Services



(a) Services and Protocols

Figure 24.6 **Elements of IEEE 802.11i**

IEEE 802.11i Services



(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure 24.6 **Elements of IEEE 802.11i**

IEEE 802.11i Phases of Operation

- Five distinct phases:

1. Discovery
2. Authentication
3. Key Management
4. Protected data transfer
5. Connection termination

IEEE 802.11i Phases of Operation

- **Five distinct phases:**

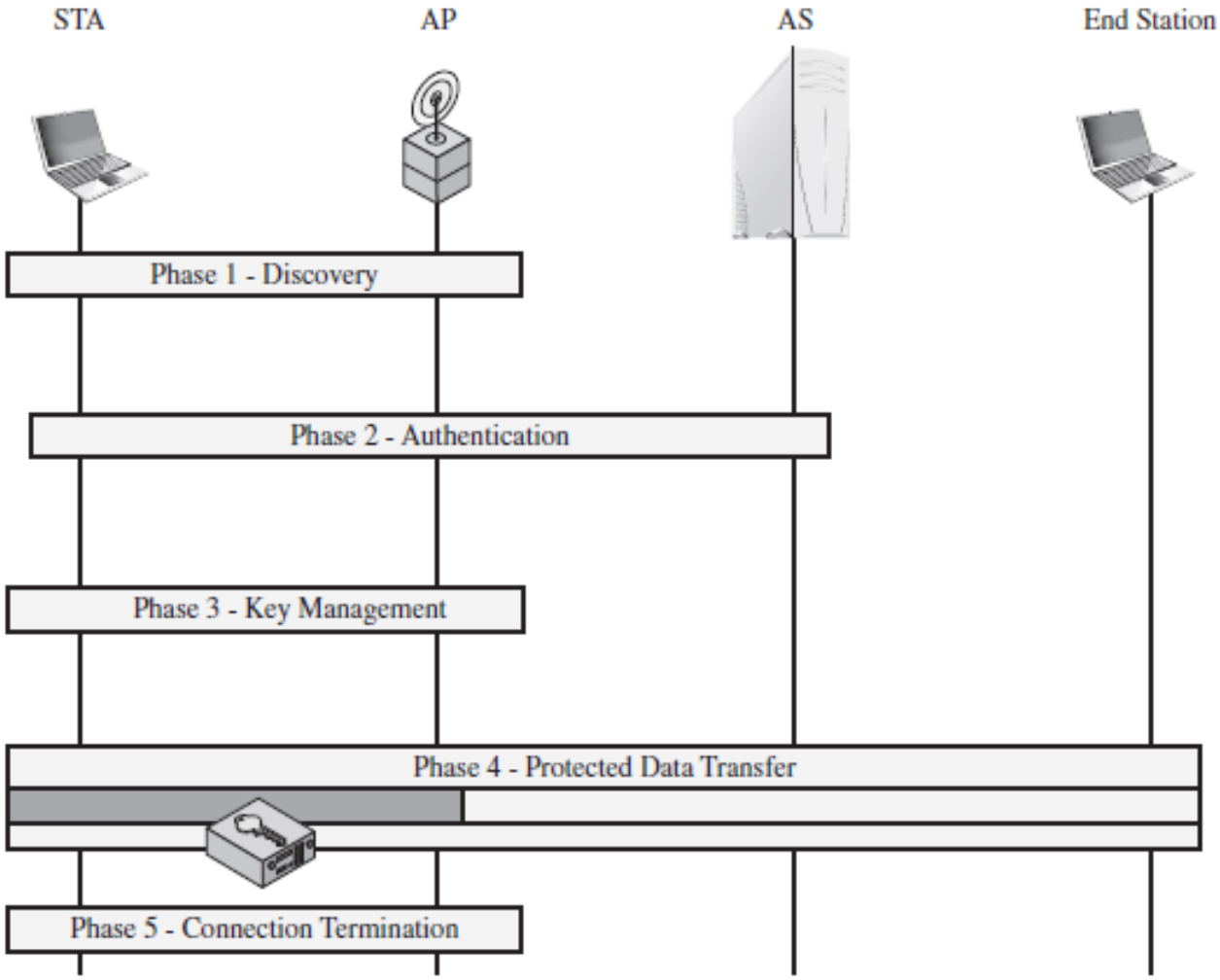


Figure 24.7 **IEEE 802.11i Phases of Operation**

IEEE 802.11i Phases of Operation

- **Discovery phase:**
  - 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 with which it wishes to communicate.
  - The STA associates with the AP to select the cipher suite and authentication mechanism when the Beacons and Probe Responses present a choice.
- **Authentication phase:**
  - The STA and AS prove their identities to each other.
  - The AP blocks non-authenticated 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

- **Key Management phase:**
  - 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.
- **Protected data transfer:**
  - Frames are exchanged between the STA and the end station through the AP.
  - Secure data transfer(encrypted) 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.