A.D. 1308
unipg

DIPARTIMENTO
DI MATEMATICA E INFORMATICA

Network Access Control and Wireless Network Security

Introduzione alla Sicurezza Informatica

Chiara Luchini

Anno Accademico 2024-2025

Network Access Control (NAC)

Network Access Control

- An umbrella term for managing access to a network
- Authenticates users logging into the network and determines what data they can access and actions they can perform
- Also examines the health of the user’s computer or mobile device

NAC elements

Access requester (AR)

Node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices.
Also referred to as **supplicants**, or **clients**.

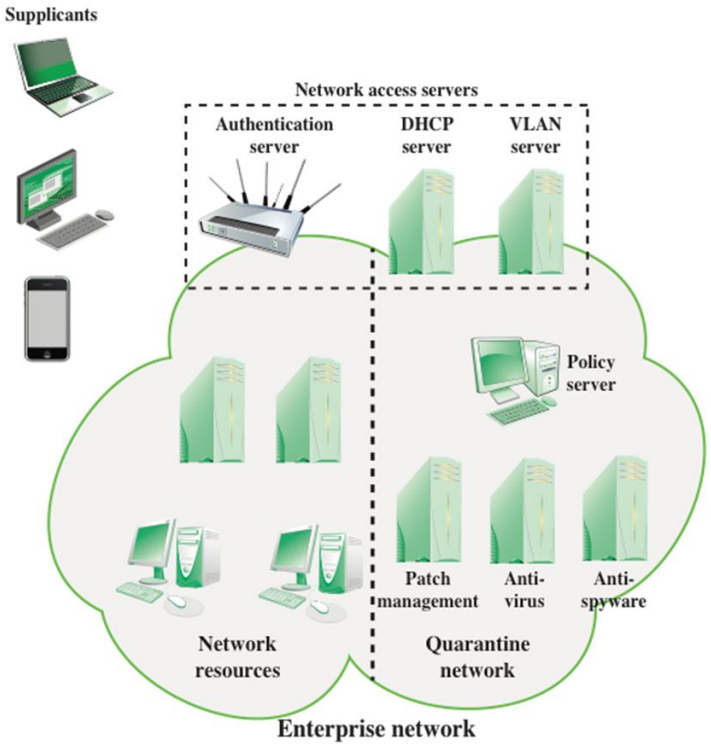
Policy Server

Determines what **access** should be granted
Often relies on backend systems

Network access server

Functions as an **access control point** for users in remote locations connecting to an enterprise's internal network
Also called a media gateway, remote access server (RAS), or policy server
May include its own authentication services or rely on a separate authentication service from the policy server

NAC elements



Network Access Enforcement Methods

The actions that are applied to ARs to regulate access to the enterprise network.
Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods

Common NAC Enforcement Methods

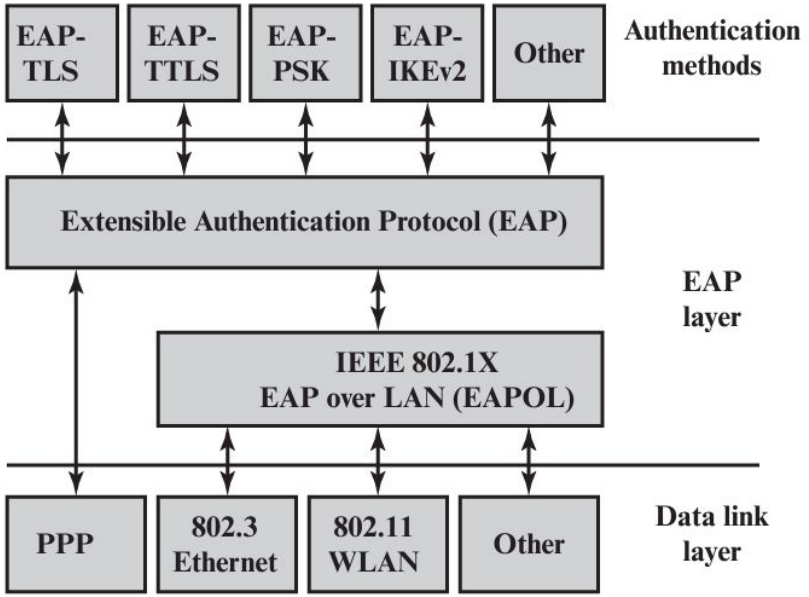
- IEEE 802.1X
- Virtual local area networks (VLANs)
- Firewall
- DHCP management

Extensible Authentication Protocol

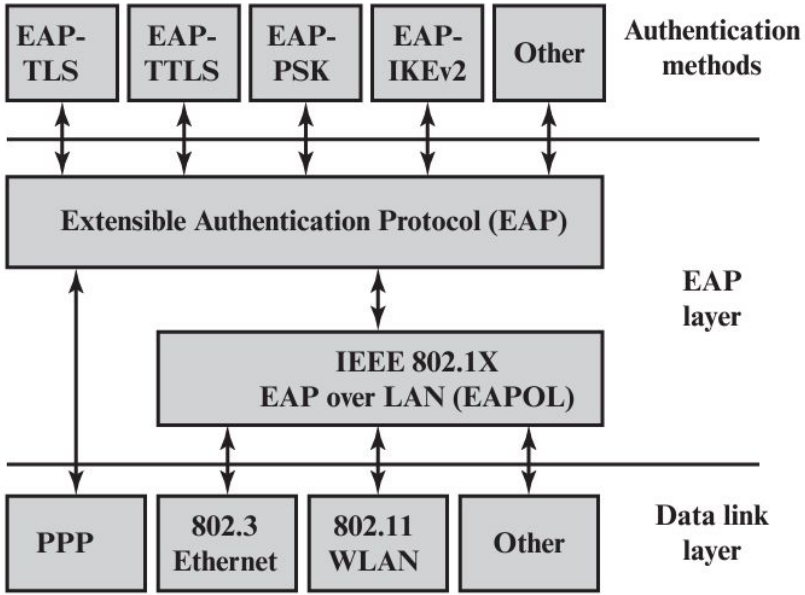
- **Extensible Authentication Protocol** (**EAP**), defined in RFC 3748, is a **framework** for network access and authentication protocols.
- EAP supports multiple authentication methods, this is why is called **extensible**.
- It provides a **generic transport service** for the exchange of authentication information between a client and an authentication server.

EAP authentication methods

- **EAP-TLS:** uses the handshake protocol in TLS. Client and server authenticate each other with digital certificates.
- **EAP-TTLS (EAP Tunneled TLS):** is like EAP-TLS, the server has a certificate to authenticate itself to the client. A secure connection (“tunnel”) is established and is used to continue the authentication by authenticating the client and possibly the server again.



EAP authentication methods

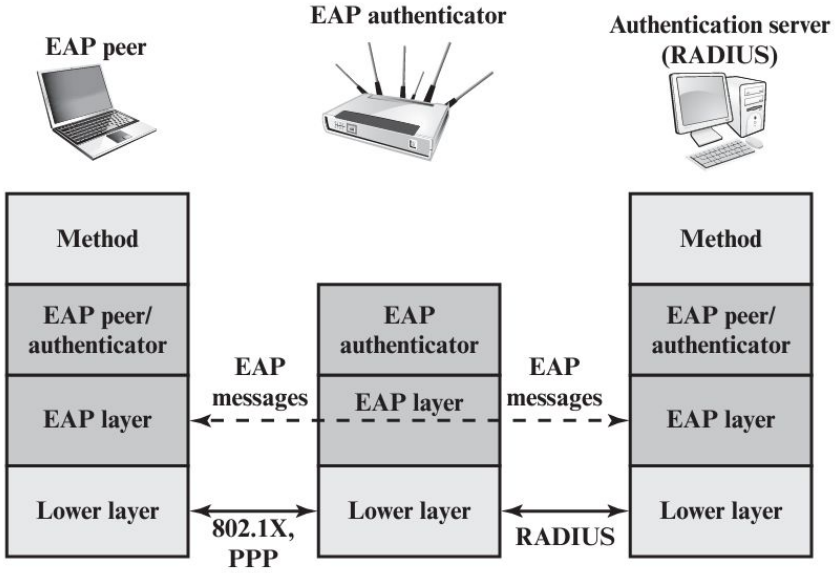


- **EAP-GPSK (Generalized Pre-Shared Key):** is an EAP method for mutual authentication and session keys derivation using Pre-Shared Key (PSK).
- **EAP-IKEv2:** is based on the **Internet Key Exchange Protocol version 2 (IKEv2)**. It supports mutual authentication and session key establishment with different methods.

EAP exchanges

A **successful authentication** is an exchange of EAP messages whereby the authenticator decides to allow access by the peer, and the peer decides to use this access.

- **EAP peer:** client computer attempting to access a network.
- **EAP authenticator:** access point or NAS needing EAP authentication before granting access.
- **Authentication server:** a Remote Authentication Dial-In User Service (RADIUS) server computer that:
  - negotiates the use of EAP method
  - validates the EAP peer's credentials
  - authorize access to the network



Remote Authentication Dial-In User Service

- RADIUS is an **AAA** (**Authentication**, **Authorization** and **Accounting**) protocol that is based on a client/server model.

- RADIUS is also a **transport protocol** for authentication mechanisms, but it can also convey other contents (RADIUS attributes) that serve specific purposes.

- Although the 802.1x standard does not specify which type of authentication server should be implemented, RADIUS is the de facto standard in 802.1x, securing the channel between Authentication Server and Authenticator.

EAP exchanges

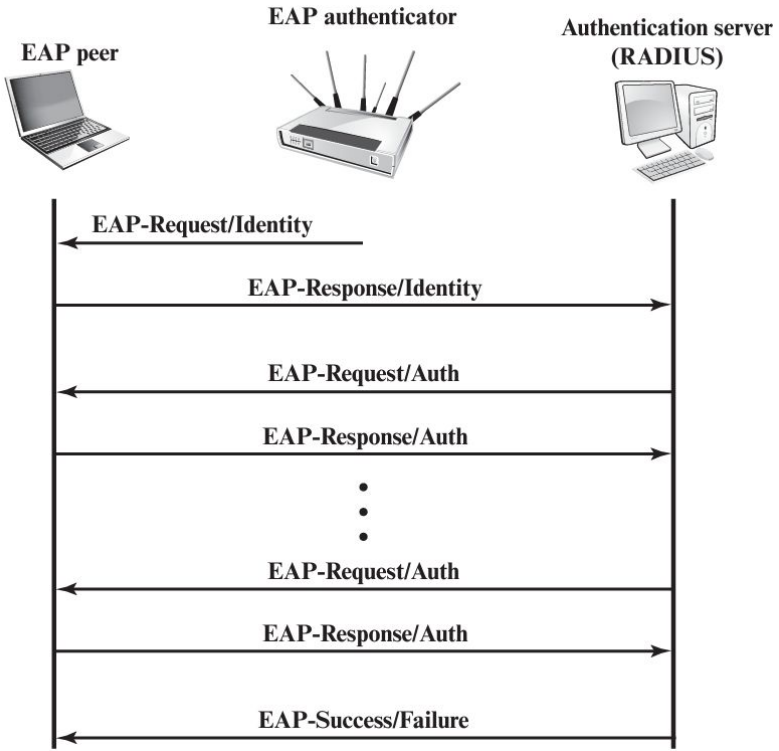
In the case where no backend authentication server is used, the EAP server is part of the authenticator. In the case where the authenticator operates in **pass-through mode**, the EAP server is located on the **backend authentication server**.

As a first step, a lower-level protocol, such as PPP (point-to-point protocol) or **IEEE 802.1X**, is used to connect to the EAP authenticator.
The software entity in the EAP peer is called **supplicant.**

EAP messages components:

- **Code:** identifies the **Type** of EAP message. The codes are Request (1), Response (2), Success (3), and Failure (4).
- **Identifier:** used to match Responses with Requests.
- **Length:** indicates the length, in octets, of the EAP message, including the Code, Identifier, Length, and Data fields.
- **Data:** contains information related to authentication. Typically, the Data field consists of a Type subfield, indicating the type of data carried, and a Type-Data field.

EAP Message Flow in Pass-Through Mode



IEEE 802.1X Port-Based Network Access Control

- Designed to provide access control functions for LANs.
- Supplicant, network access point and authentication server correspond to peer, authenticator and authentication server.

Authenticator
An entity at one end of a point-to-point LAN segment that facilities authentication of the entity to the other end of the link.

Authentication exchange
The two-party conversation between systems performing an authentication process.

Authentication process
The cryptographic operations and supporting data frames that perform the actual authentication.

Authentication server (AS)
An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by supplicant, whether the supplicant is authorized to access the services provided by the system in which the authenticator resides.

Authentication transport
The datagram session that actively transfers the authentication exchange between two systems.

Bridge port
A port of an IEEE 802.1D or 802.1Q bridge.

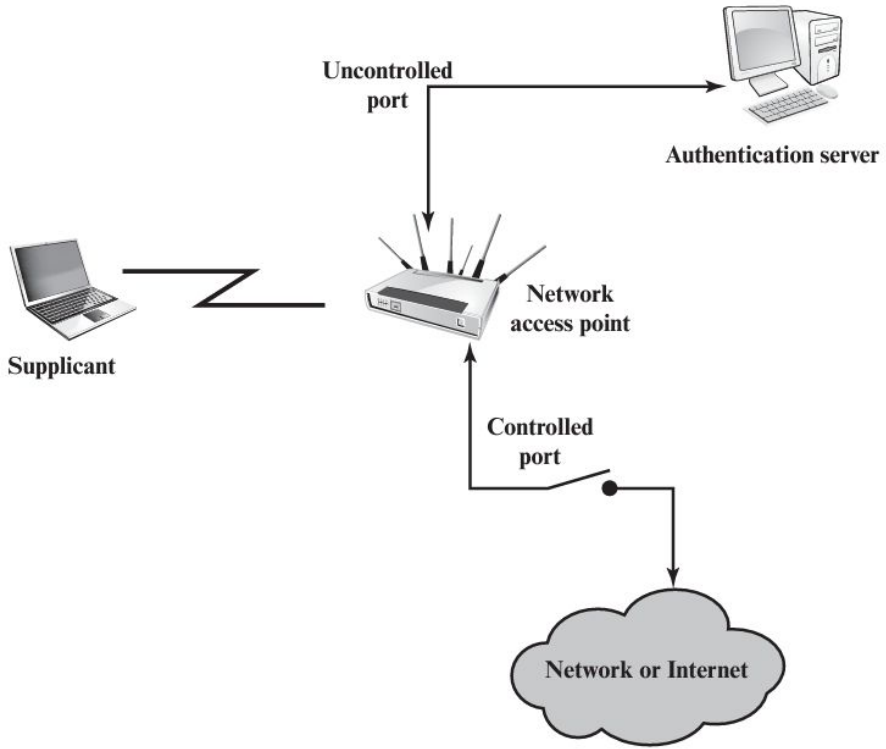
Edge port
A bridge port attached to a LAN that has no other bridges attached to it.

Network access port
A point of attachment of a system to a LAN. It can be a physical port, such as a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.

Port access entity (PAE)
The protocol entity associated with a port. It can support the protocol functionality associated with the authenticator, the supplicant, or both.

Supplicant
An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link.

802.1X Access Control



- Uses **controlled** and **uncontrolled** ports.
- Ports are **logical entities** defined within the authenticator and refer to physical network connections.
- Uncontrolled port allows the exchange of **protocol data units** (**PDUs**) between supplicant and AS, even if the supplicant is not authenticated.
- **Controlled port** allows the exchange of PDUs between a supplicant and other systems in the network only if the supplicant is **authorized**.

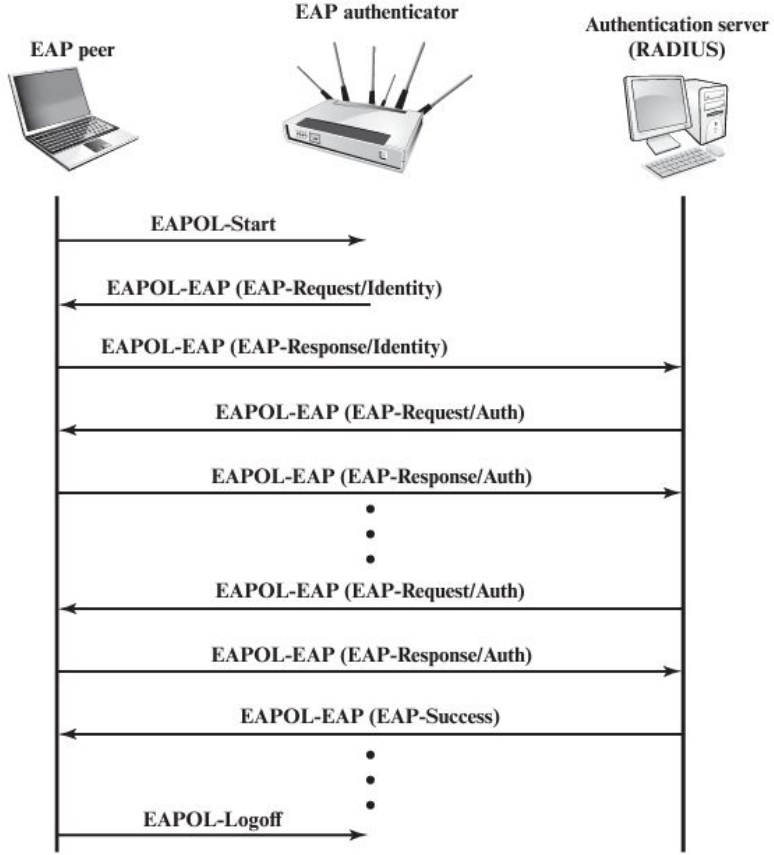
EAP over LAN

- EAPOL operates at the **network layers** and makes use of an **IEEE 802 LAN**, such as Ethernet or Wi-Fi, at the link level.
- EAPOL enables a supplicant to communicate with an authenticator and supports the exchange of EAP packets for authentication.

Frame Type	Definition
EAPOL-EAP	Contains an encapsulated EAP packet.
EAPOL-Start	A supplicant can issue this packet instead of waiting for a challenge from the authenticator.
EAPOL-Logoff	Used to return the state of the port to unauthorized when the supplicant is finished using the network.
EAPOL-Key	Used to exchange cryptographic keying information.

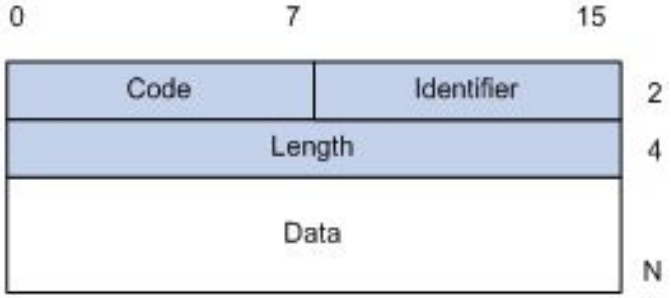
EAPOL flow

- When the supplicant first connects to the LAN, it does not know the MAC address of the authenticator.
- **EAPOL-Start** packet: is sent to a special group-multicast address reserved for IEEE 802.1X authenticators. A supplicant can determine whether an authenticator is present and let it know that the supplicant is ready.
- The authenticator sends an **EAP-Request Identity** message encapsulated in an **EAPOL-EAP** packet.
- The authenticator uses the **EAP-Key** packet to send cryptographic keys to the supplicant once it has decided to admit it to the network.
- **EAP-Logoff** packet: the supplicant wishes to be disconnected from the network.

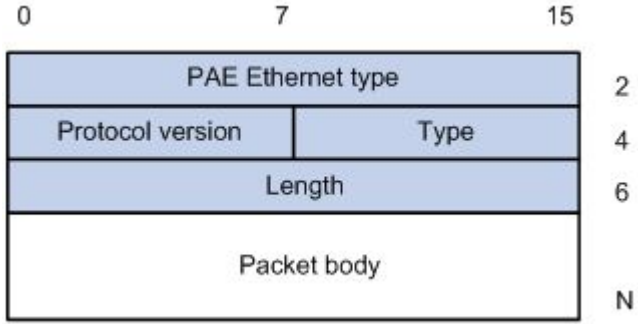


EAPOL packet format

- **Ethernet type:** Protocol type. It takes the value 0x888E for EAPOL.
- **Protocol version:** version of EAPOL.
- **Packet type:** indicates start, EAP, key, logoff, etc.
- **Packet body length:** If the packet includes a body, this field indicates the body length.
- **Packet body:** The payload for this EAPOL packet. An example is an EAP packet.



EAP Packet



EAPOL Packet

Wireless Network Security

Wireless Security

Wireless environments have 3 components that can be a point of attack:

- **Wireless client (endpoint):** can be a cellphone, laptop or tablet, a wireless sensor...
- **Wireless access point:** provides a connection to network or service.
- **Wireless medium:** transmission that carries the radio waves for data transfer.

Wireless Security

Key factors contributing to security risks:

- **Channel:** usage of broadcasting communication which are susceptible to eavesdropping, jamming and active attacks.
- **Mobility:** wireless devices are more portable and mobile.
- **Resources:** wireless devices have limited memory and processing resources with which to counter threats like DDoS and malware.
- **Accessibility:** wireless devices, like sensors and robots, may be left unattended in remote and/or hostile locations. This greatly increases their vulnerability to physical attacks.

Wireless Network Threats

Accidental Association

A user intending to connect to one LAN may unintentionally lock on to a wireless access point from a neighboring network.

Malicious Association

A wireless devices appearing like a legitimate access point that steals passwords users and penetrate a wired connection.

Ad hoc networks

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

Nontraditional networks and links, such as personal network Bluetooth devices, and barcode readers, pose a security risk in terms of both eavesdropping and spoofing.

Wireless Network Threats

Identity theft (MAC spoofing)

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

Persuasion of 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.

Denial of service (DoS)

A DoS attack occurs when an attacker continually bombards a wireless access point or wireless port with various protocol messages designed to consume system resources.

Network injection

Wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages.

Securing Wireless Transmissions

The principal threats to wireless transmission are **eavesdropping**, **altering or inserting messages**, and **disruption.** To deal with eavesdropping, two types of countermeasures are appropriate:

- **Signal-hiding techniques**
  - Turn off service set identifier (SSID) broadcasting by wireless access points
  - Assign cryptic names to SSIDs
  - Reduce signal strength to the lowest level that still provides requisite coverage
  - Locate wireless access points in the interior of the building, away from windows and exterior walls
- **Encryption**
  - Is effective against eavesdropping to the extent that the encryption keys are secured

Securing Wireless Access Points

- The main threat involving wireless access points is **unauthorized access** to the network
- The principal approach for preventing such access is the **IEEE 802.1x** standard for **port-based network access control**
  - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
  - The use of 802.1x can prevent rogue access points and other unauthorized devices from becoming insecure backdoors

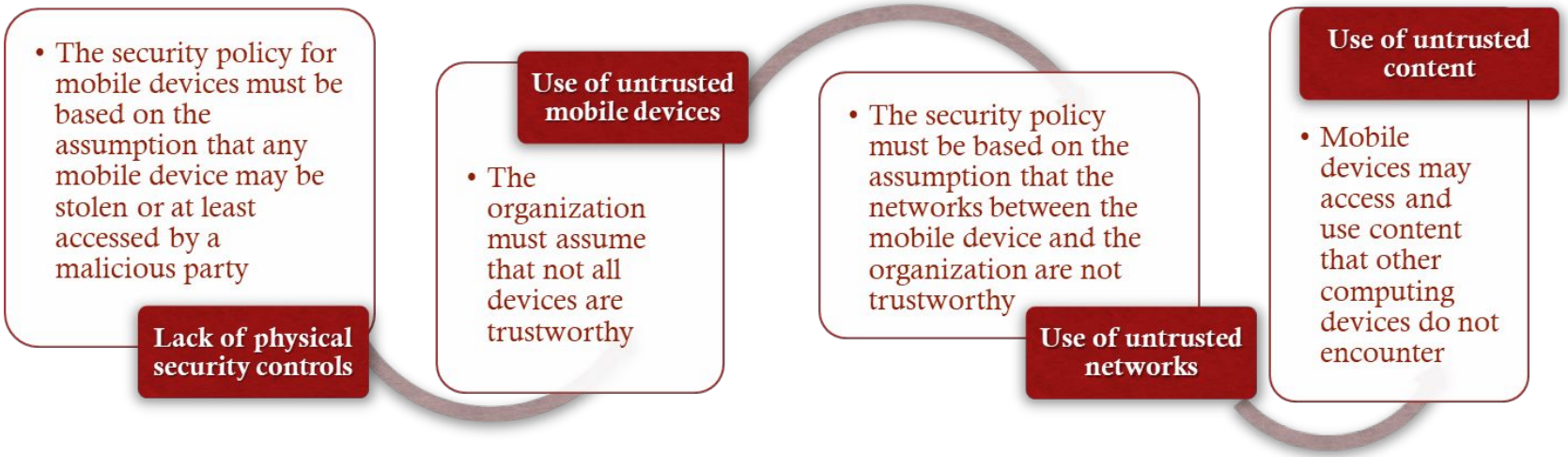
Securing Wireless Networks

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

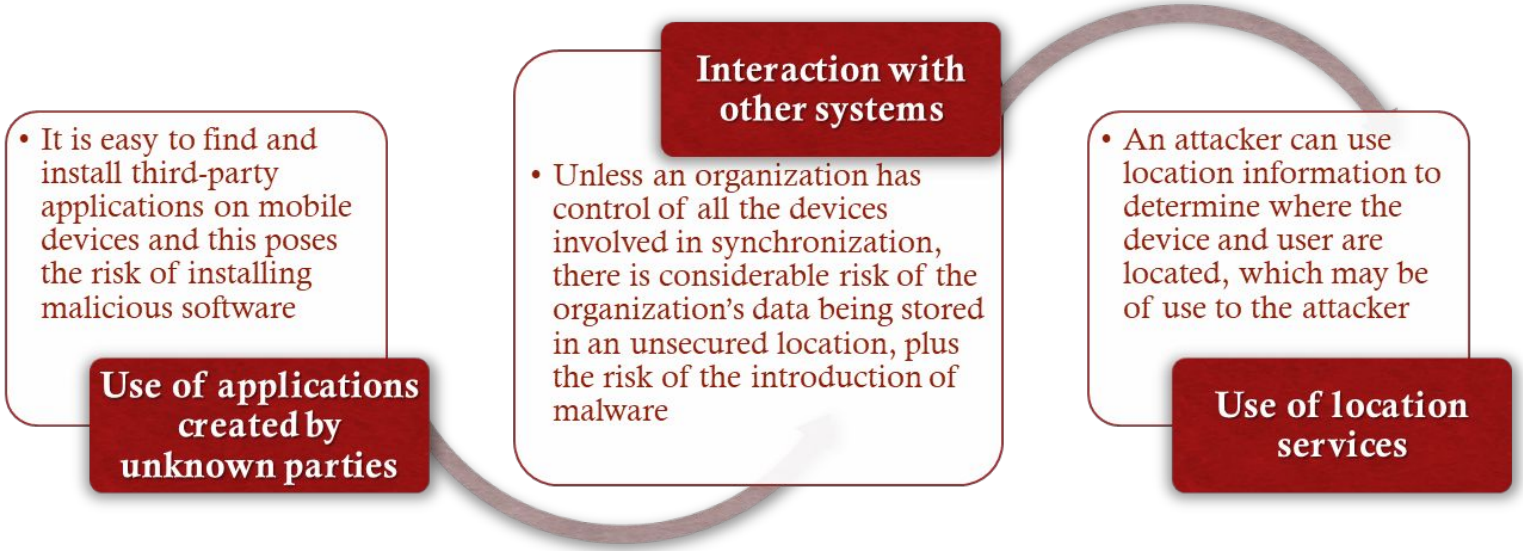
Mobile Device Security

- Mobile devices have become an **essential element for organizations** as part of the overall network infrastructure
- Prior to the widespread use of smartphones, network security was based upon clearly **defined perimeters** that separated trusted internal networks from the untrusted Internet
- Due to massive changes, an organization's networks must now accommodate:
  - Growing use of new devices
  - Cloud-based applications
  - De-perimeterization
  - External business requirements

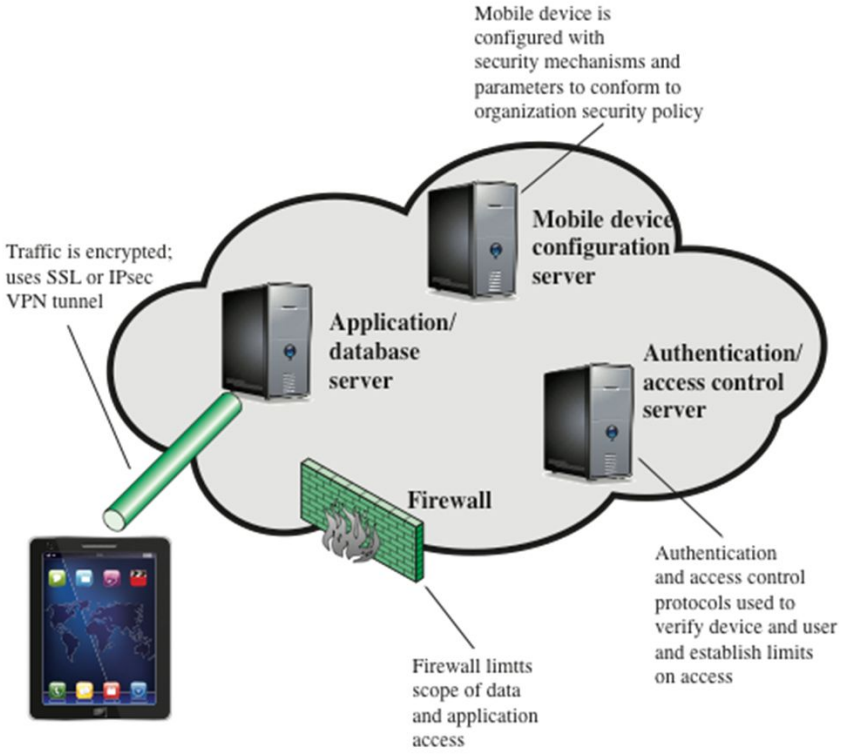
Security Threats



Security Threats



Mobile Device Security Elements



Wireless network

Wireless (“without wire”) information is transmitted **“over the air”**.

Types of wireless networks can be:

- WPAN (Wireless Personal Area Network), at home level
- WLAN (Wireless Local Area Network) properly known as Wi-fi.
- Wireless WAN (Wide Area Network).
- WMAN (Wireless Metropolitan Area Network)
- BWA (Broadband Wireless Access), which is experiencing widespread diffusion thanks to WiMAX technology

to these are added:

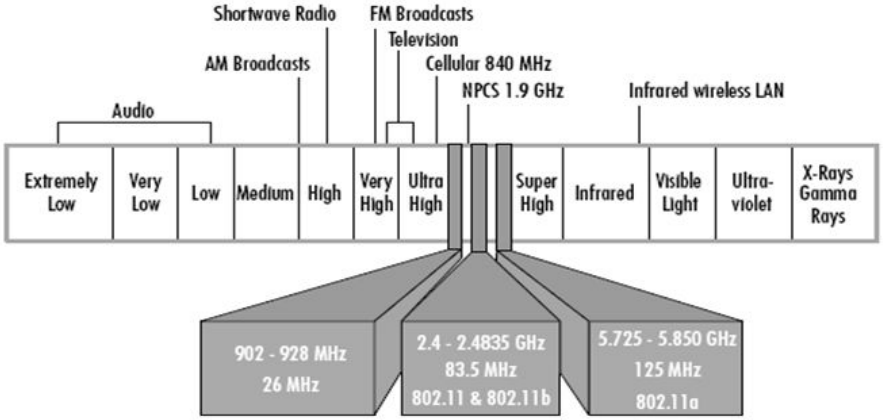
- Mobile cellular networks such as GSM, GPRS, EDGE, UMTS, HSPA, LTE.
- Satellite networks

Wireless network

WLAN = **Wireless LAN** opposed to wired LAN
The three main problems inherent in the wired LAN model:

- Costs
- Limitations on distances covered by cabling
- Inability to implement the mobility of user workstations

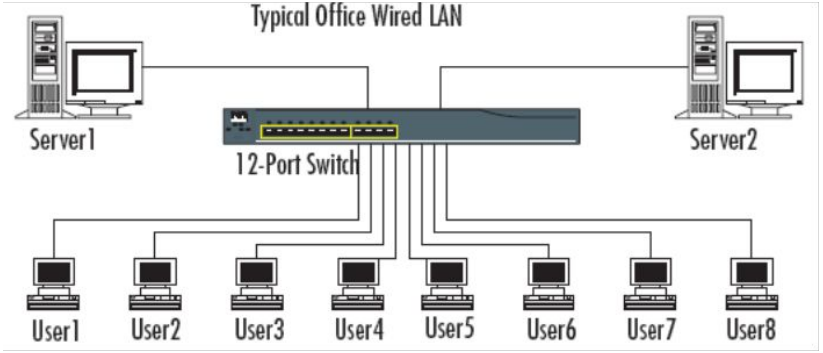
addressed and resolved in Wireless LANs.
With **WLANs** the physical medium changes, **radio waves** are used in the free bands (no licenses required) defined as **ISM** (**2.4GHz or 5GHz**) and the method of access to the medium is **CSMA/CA**.

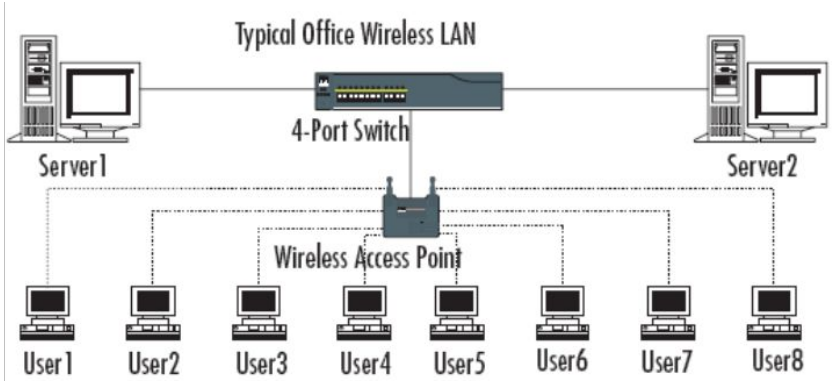


The greatest concern arises from the fact that over-the-air transmission is in all respects a **broadcast transmission**.

Advantages of Wireless

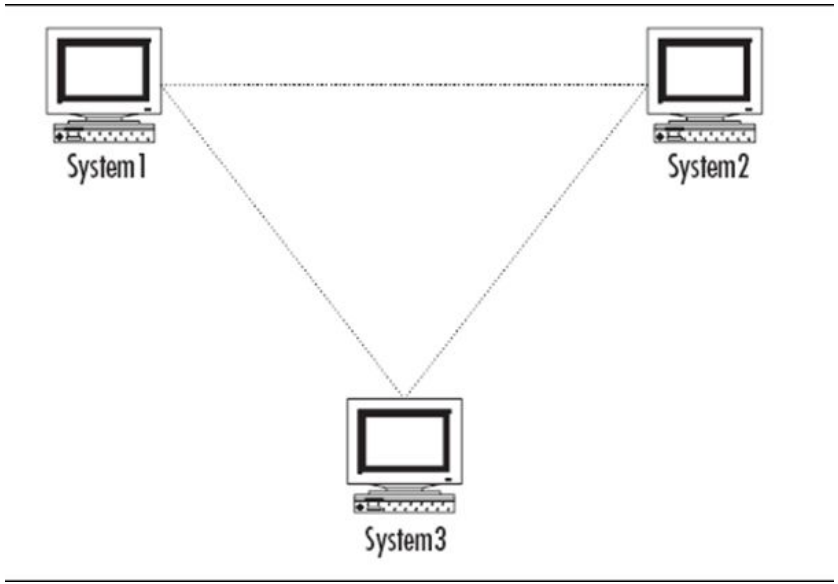
- Reduced costs
- Fewer problems related to distances (use of multiple APs or wireless relaying)
- Mobility of network stations





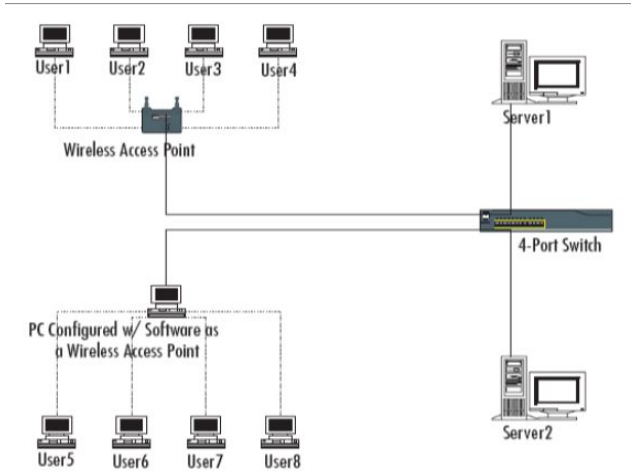
Ad hoc mode (or peer to peer)

Computers can communicate directly with each other only through their own wireless network interface



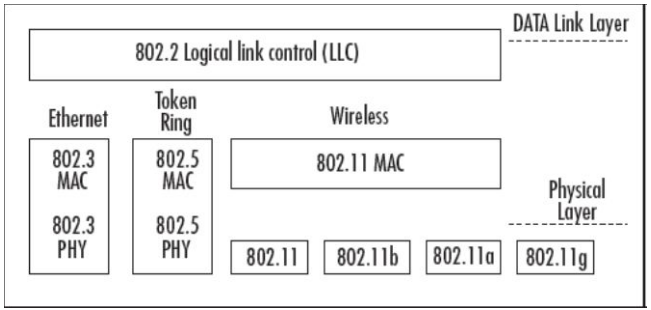
WLAN operating modes

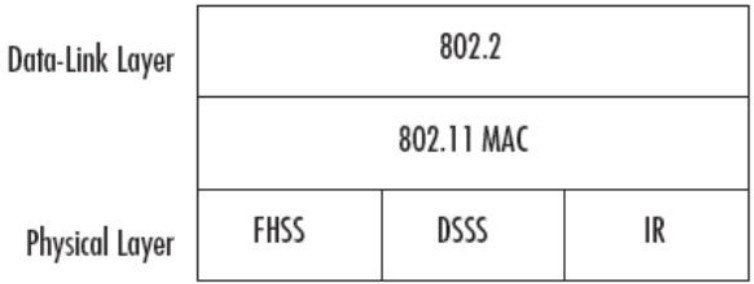
Network communication takes place thanks to hardware or software **Access Points (APs)** that are an integral part of the WLAN network, and through **wireless network interfaces** installed and configured on each workstation in order to communicate with specific APs to connect to specific WLANs



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
- The new standardization compared to the Ethernet case imposes variations in the structure of the information that is transmitted over the network, therefore a new format for the Frames.





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 802.11b

- After the ratification of IEEE 802.11 which operated with a maximum speed of **2Mbps**, an increase in transmission speed became necessary.

- At the end of 1999, IEEE 802.11b was issued which operates in the **2.4 GHz** band and reaches **11 Mbps** thanks to the **Direct Sequence Spread Spectrum (DSSS)** type signal modulation which allows for **11 effective transmission channels**, of which 3 are non-overlapping (1,6 and 11), therefore immune to interference.

IEEE 802.11a

- As increasingly higher transmission speeds are required, especially to satisfy audio/video streaming needs, **IEEE 802.11a** was issued which reaches **54 Mbps** operating in the 5 GHz band with a new **Orthogonal Frequency Division Multiplexing (OFDM)** type signal modulation which allows to have 12 non-overlapping transmission channels.

- The 5 GHz band in Europe is used by **satellite** and **military communications**, so two further measures are introduced here: **Dynamic Frequency Selection (DFS)** and **Transmit Power Control (TPC)**

- The extension of the coverage area is approximately half that of IEEE 802.11b and the same considerations apply to the variation of transmission speed with distance. While on the one hand this entails higher costs for the same coverage, it has the advantage of having greater bandwidth for all network stations as the transmission speed is significantly higher.

IEEE 802.11g and now

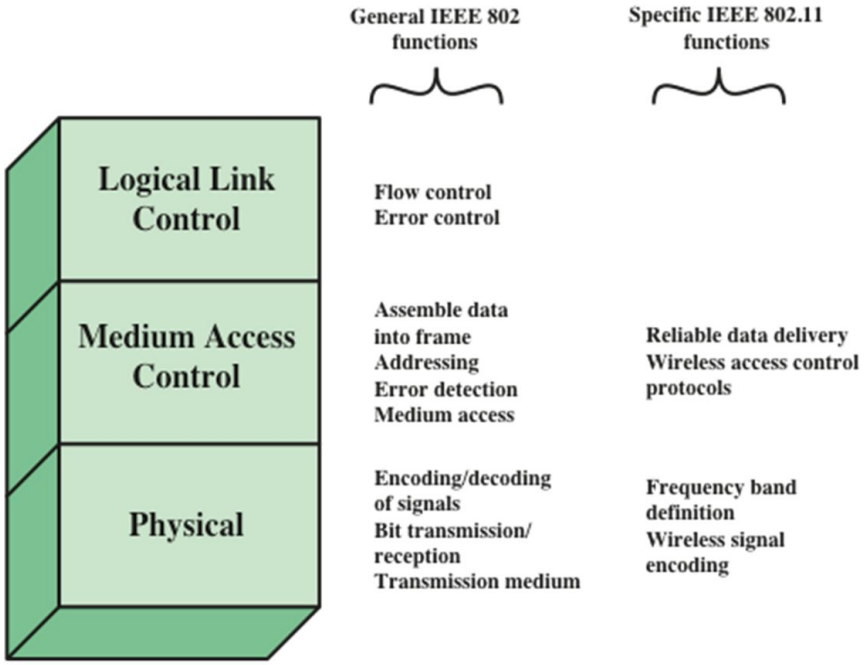
- Given the problems linked to the previous standard, in 2003 IEEE 802.11g was issued which reaches **54 Mbps** operating in the **2.4 GHz** band, with the same signal modulation as IEEE 802.11a (OFDM).
- The extension of the coverage area is smaller than that of IEEE 802.11b but larger than that of IEEE 802.11a.
- One of the strengths of this standard is its compatibility with IEEE 802.11b.

802.11be (Wi-Fi 7)

IEEE 802.11be Extremely High Throughput (EHT) is the potential next amendment to the 802.11 IEEE standard, and will likely be designated as Wi-Fi 7. It will build upon 802.11ax, focusing on WLAN indoor and outdoor operation with stationary and pedestrian speeds in the 2.4 GHz, 5 GHz, and 6 GHz frequency bands.

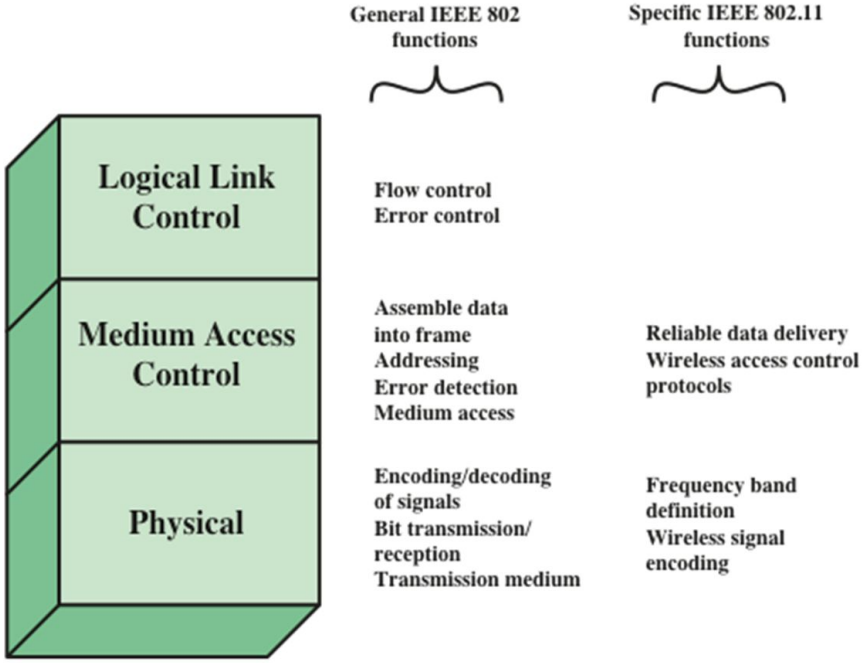
IEEE 802.11 Protocol Stack

- **Physical Layer:** lowest layer that includes:
  - encoding/decoding signals
  - bit transmission/reception
  - specification for transmission medium
  - frequency bands and antenna characteristics



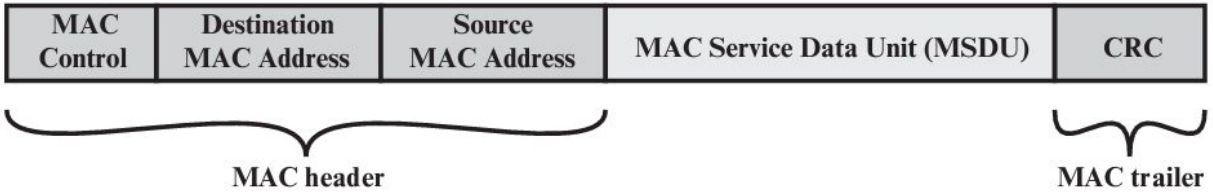
IEEE 802.11 Protocol Stack

- **Media Access Control (MAC):** receives data, in the **MAC service data unit (MSDU)** format, from higher-layer protocol like **Logical Link Control (LLC)** layer.
  Functions:
  - On transmission, assemble data into **MAC protocol data unit (MPDU)** frame with address and error-detection fields.
  - On reception, disassemble frame, and perform address recognition and error detection.
  - Govern access to the LAN transmission medium.



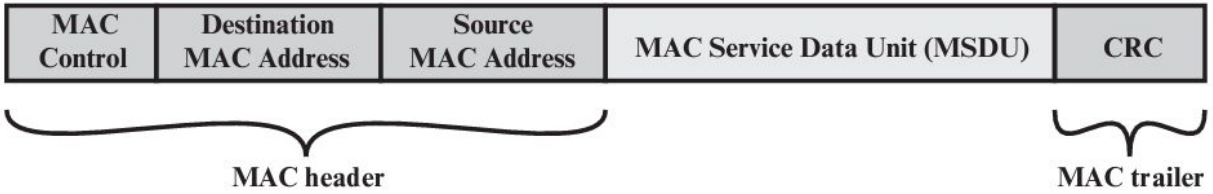
MAC protocol data unit (MPDU)

- **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.



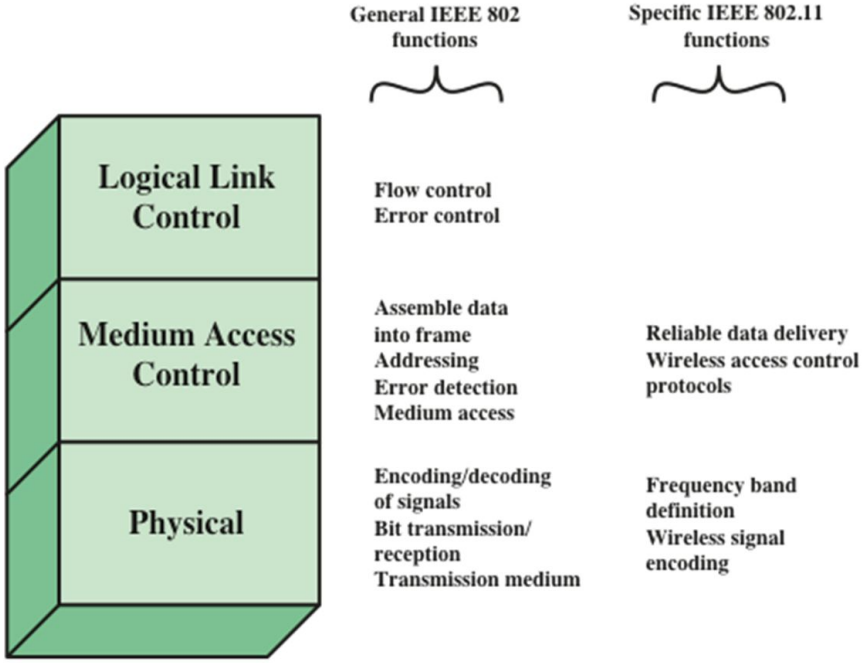
MAC protocol data unit (MPDU)

- **MAC Service Data Unit:** The data from the next higher layer.
- **Cyclic Redundancy Check (CRC):** also known as the **Frame Check Sequence (FCS)** field. This is an **error-detecting code** that 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.



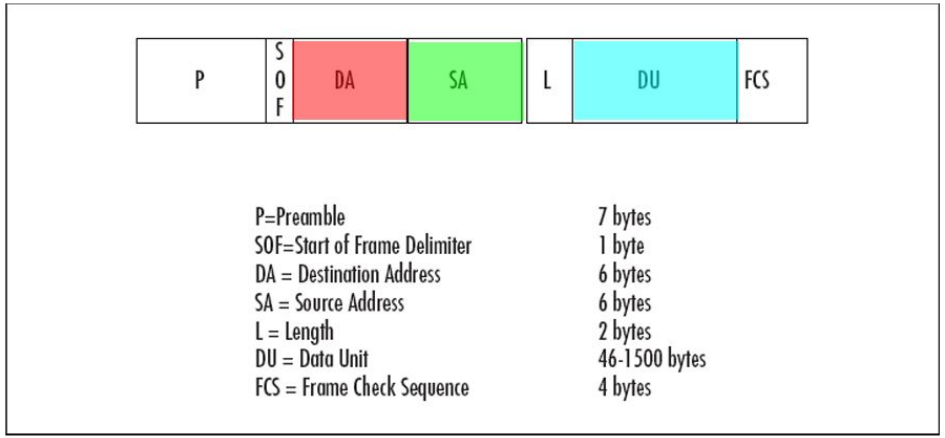
IEEE 802.11 Protocol Stack

- **Logical Link Control (LLC):** the data-link protocol entity is responsible not only for **detecting errors** using the **CRC**, but for **recovering** from those errors by retransmitting damaged frames. In the LAN protocol architecture, these two functions are split between the MAC and LLC layers. The MAC layer is responsible for detecting errors and discarding any frames that contain errors. The LLC layer optionally keeps track of which frames have been successfully received and retransmits unsuccessful frames.



Frame Ethernet IEEE 802.3

- The **SA** field contains the MAC Address of the **Frame Sender**
- The **DA** field contains the MAC Address of the **Frame Recipient**
- The **DU** field contains the actual **“data”** of the transmission

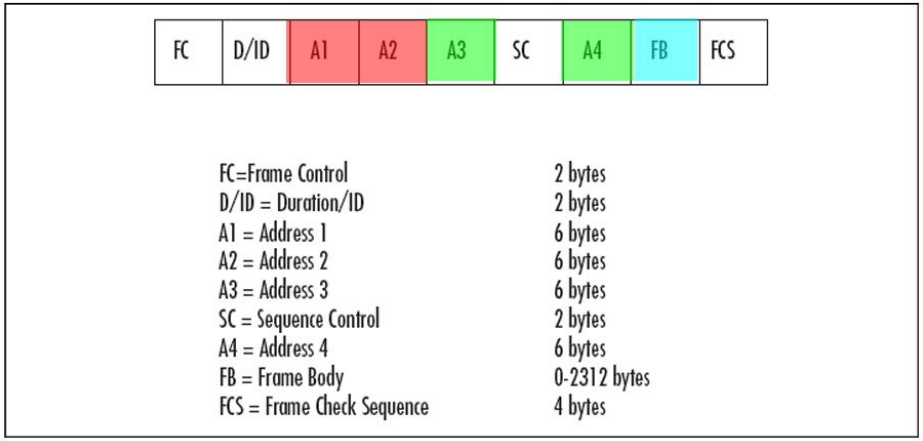


Frame Wireless IEEE 802.11b

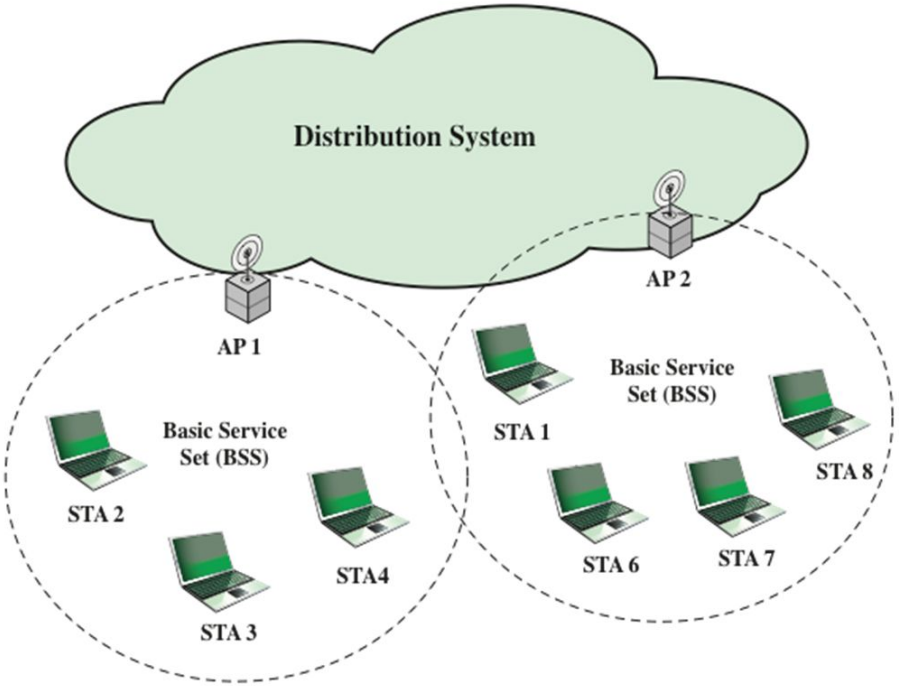
Just two addresses are no longer sufficient to track information transmissions due to the possible presence of particular intermediate nodes in the network, so up to **4 address fields** are provided **(A1,...,A4)** always containing a MAC Address which can be:

- of the **Access Point (AP)**
- of the **Sender (TA)**
- of the first **receiver** in the WLAN network **(RA)**,
- of the **transmitter** in the WLAN network **(SA)**
- of the **Recipient of the Frame (DA)**

The FB field contains the actual "data" of the transmission



IEEE 802.11 Extended Service Set



- **Basic Service Set (BSS):** wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium.
- **Distribution System (DS):** system used to interconnect a set of BSS and integrated LANs to create an ESS.
- **Extended Service Set (ESS):** two or more basic services sets interconnected by a DS.
- **Access Point (AC):** functions as a bridge and a relay point. It provides access to the DS via the wireless medium for the stations.

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
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

Distribution of Messages Within a DS

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

1. **Integration**
   a. Enables transfer of data between a station on an IEEE 802.11 LAN and a station on an integrated IEEE 802.x LAN
   b. Takes care of any address translation and media conversion logic required for the exchange of data
2. **Distribution**
   a. The primary service used by stations to exchange MPDUs when the MPDUs must traverse the DS to get from a station in one BSS to a station in another BSS

Association-Related Services

Associated-related services provide information about stations within the ESS. Stations must be **associated** before the DS delivers data to or accept from it. Transition types based on mobility:

1. **No transition**
   a. A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS
2. **BSS transition**
   a. This is defined as a station movement from one BSS to another BSS within the same ESS
   b. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station
3. **ESS transition**
   a. This is defined as a station movement from a BSS in one ESS to a BSS within another ESS
   b. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed
   c. Disruption of service is likely to occur

Association-Related Services

To deliver a message within a DS, the distribution service needs to know the **identity of the AP** to which the message should be delivered in order for that message to reach the **destination station.**

Three services relate to a station maintaining an association with the AP within its current BSS:

1. **Association**
   a. Establishes an initial association between a station and an AP
2. **Reassociation**
   a. Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another
3. **Disassociation**
   a. A notification from either a station or an AP that an existing association is terminated

IEEE 802.11i Wireless LAN Security

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

Wired Equivalent Privacy (WEP)

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

Wi-Fi Protected Access (WPA)

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

Robust Security Network (RSN)

- Final form of the 802.11i standard
- Complex

Wi-Fi Protected Access (WPA)

WEP is a weak protocol: it can be broken in 15 minutes!

The weaknesses of WEP arise from the relative static nature of the shared key and a weak or non-existent system of authentication.

Working Group 11 of the 802 Committee remedied this by issuing the **IEEE 802.11i** standard with which it proposes a new, more robust and secure **framework** for WLANs.

Before the standard was completed and issued, the **Wi-Fi Alliance** tried to address the security emergency caused by WEP by introducing **WPA** which partially implements the IEEE 802.11i standard:

- Improvements in data integrity:
- **128-bit key** for the RC4 algorithm and **48-bit** initialization vector
- Cryptographic keys are changed periodically (**TKIP**)
- Possibility to use the **802.1x Authentication Protocol**

IEEE 802.11i (WPA2)

The **IEEE 802.11i** standard, issued in 2004, after WPA, is also known by the acronym **WPA2** to distinguish it from WPA.

WPA2 completely remedies the flaws of WEP by acting on various fronts:

- Dynamic management of cryptographic key exchange using **Temporal Key Integrity Protocol (TKIP)**
- Improved communication integrity thanks to **Counter mode with CBC-MAC Protocol (CCMP)**
- Improving communication confidentiality through **Advanced Encryption System (AES)** encryption
- Network access control using **802.1x Authentication**

Elements of IEEE 802.11i

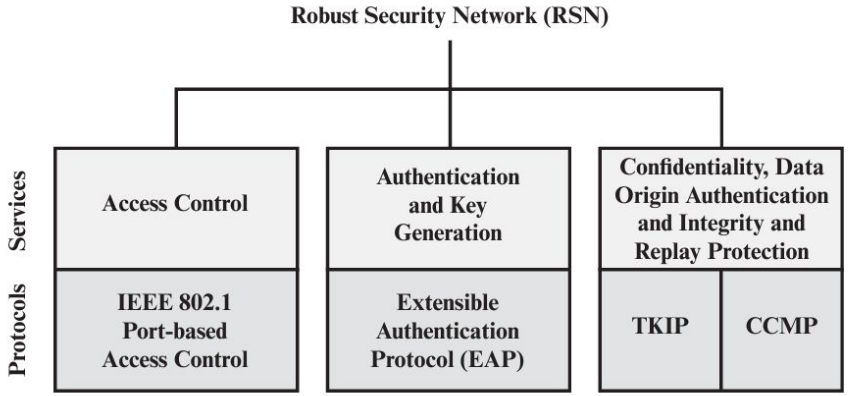
The 802.11i RSN security specification defines the following services.

- **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.

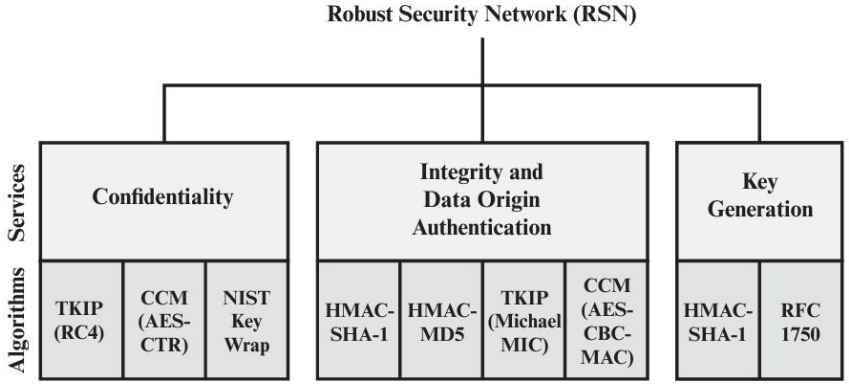
- **Access control:** This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.

- **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.

Elements of IEEE 802.11i



(a) Services and protocols



(b) Cryptographic algorithms

CBC-MAC = Cipher 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

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.

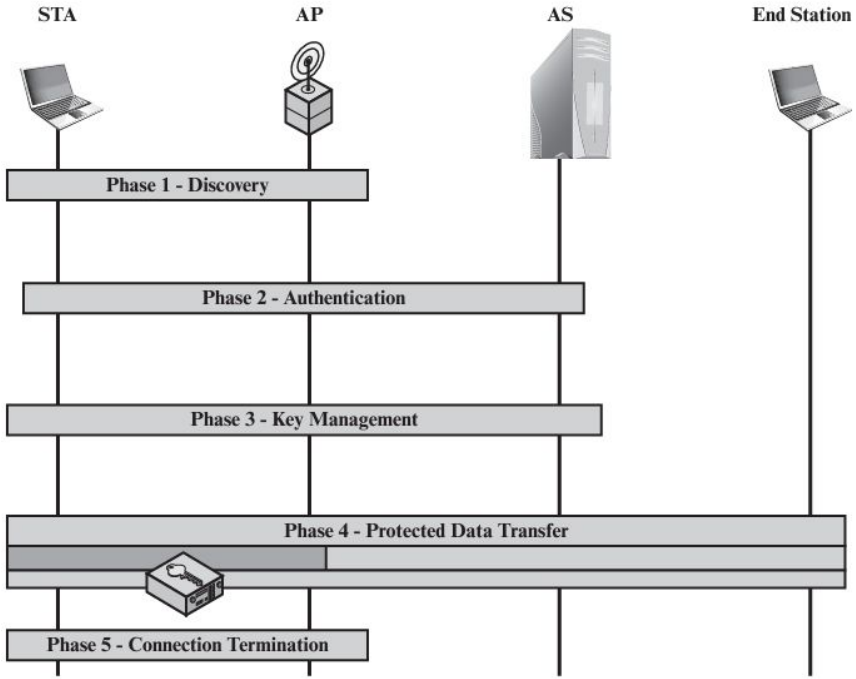
3. Two wireless stations in different BSSs communicating via their respective APs across a distribution system.

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

One new component is the **authentication server (AS)**. The rectangles indicate the exchange of sequences of MPDUs. The five phases are defined as follows.

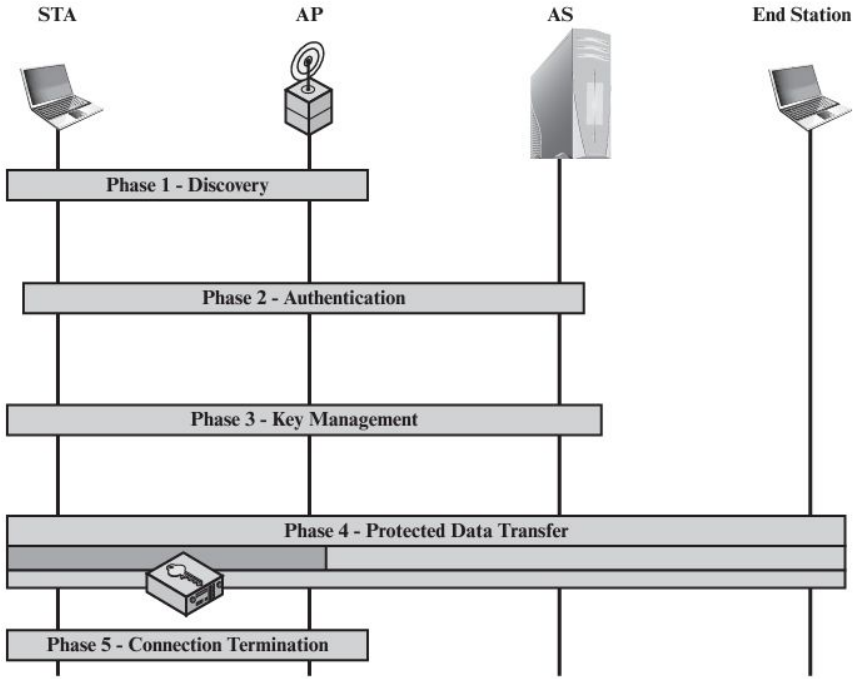
- **Discovery:** An AP uses messages called Beacons and Probe responses to advertise its IEEE 802.11i security policy.
- **Authentication:** During this phase, the STA and AS prove their identities to each other.
- **Key generation and distribution:** The AP and the STA perform several operations that cause cryptographic keys to be generated and placed on the AP and the STA. Frames are exchanged between the AP and STA only.

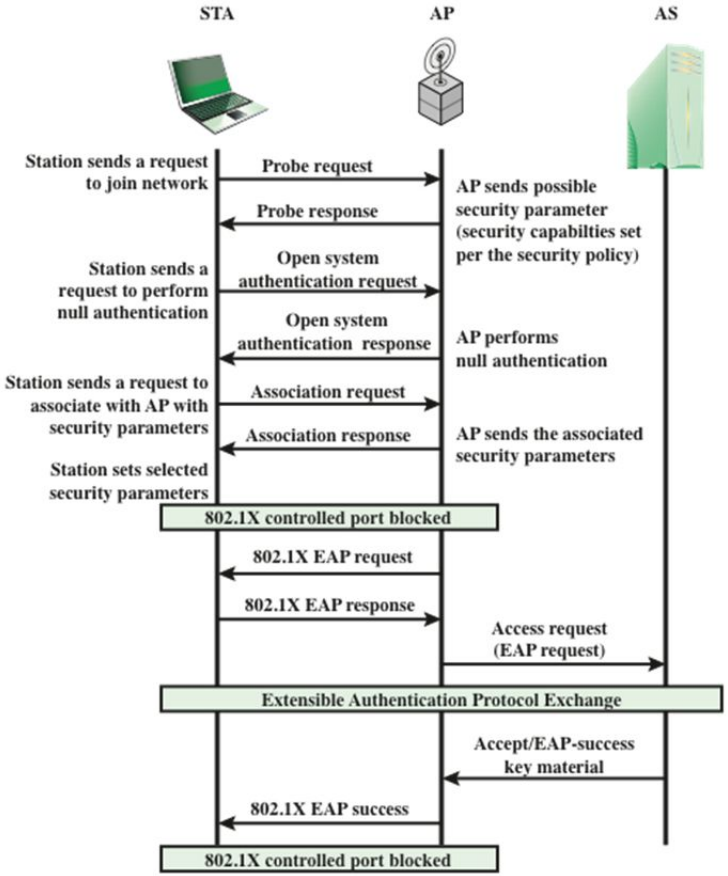


IEEE 802.11i Phases of Operation

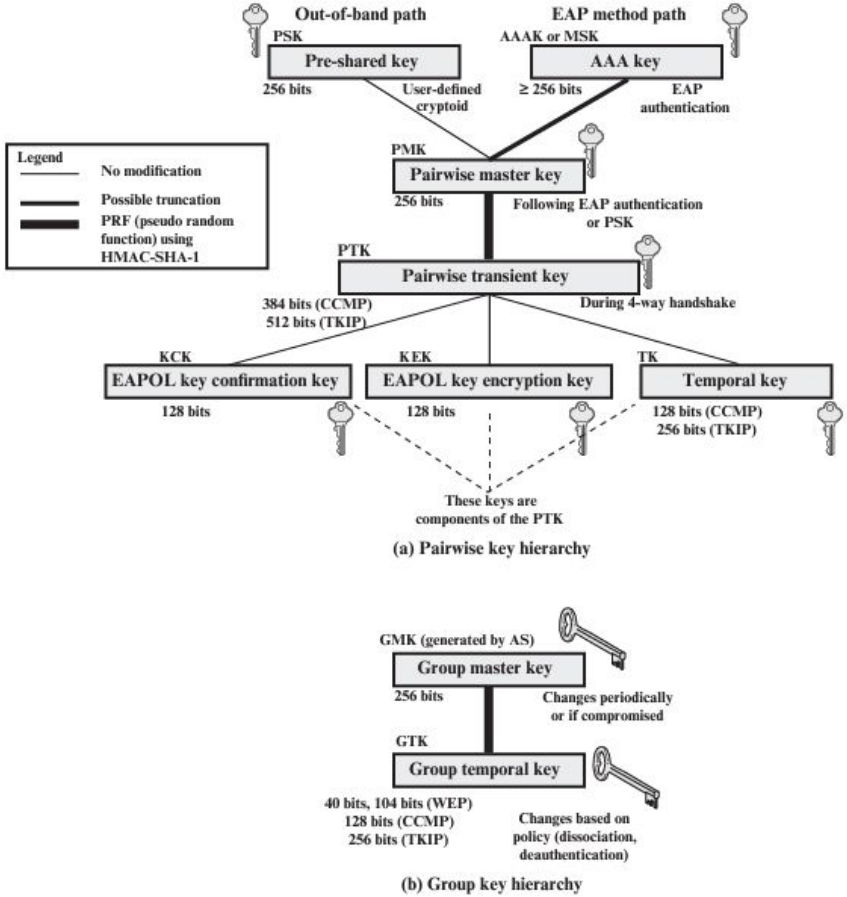
- **Protected data transfer:** Frames are exchanged between the STA and the end station through the AP. As denoted by the shading and the encryption module icon, secure data transfer occurs between the STA and the AP only; security is not provided end-to-end.

- **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





IEEE 802.11i Phases of Operation: Capability DIscovery, Authentication and Association



IEEE 802.11i Key Hierarchies

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 Keys for Data Confidentiality and Integrity Protocols

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

EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK)

Supports the **integrity** and data origin **authenticity** of STA-to-AP control frames during operational setup of an RSN
It also performs an access control function: **proof-of-possession** of the PMK
An entity that possesses the PMK is authorized to use the link

EAPOL Key Encryption Key (EAPOL-KEK)

Protects the confidentiality of keys and other data during some RSN association procedures

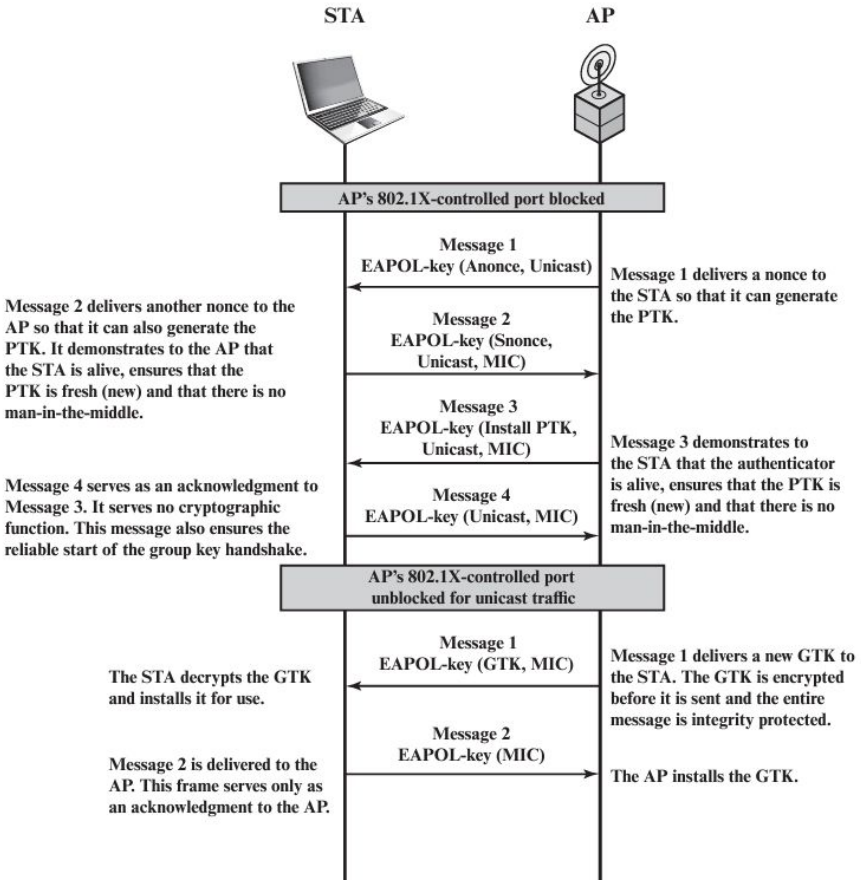
Temporal Key (TK)

Provides the actual protection for user traffic

Group Keys

Group keys are used for multicast communication in which one STA sends MPDUs to multiple STAs

- **Group master key (GMK)**
  - Key-generating key used with other inputs to derive the GTK
- **Group temporal key (GTK)**
  - Generated by the AP and transmitted to its associated STAs
  - IEEE 802.11i requires that its value is computationally indistinguishable from random
  - Distributed securely using the pairwise keys that are already established
  - Is changed every time a device leaves the network



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

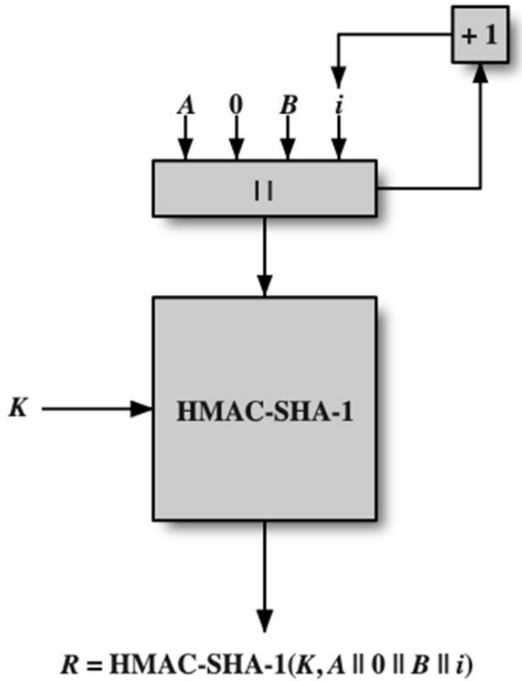
Protected Data Transfer Phase

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

- **Temporal Key Integrity Protocol (TKIP)**
  - Designed to require only software changes to devices that are implemented with WEP
  - Provides two services:
    - Message integrity: adds a MIC to the 802.11 MAC frame
    - Data confidentiality: encryption of MPDU plus MIC value using RC4
- **Counter Mode-CBC MAC Protocol (CCMP)**
  - Intended for newer IEEE 802.11 devices that are equipped with the hardware to support this scheme
  - Provides two services:
    - Message integrity: uses cipher block chaining message authentication code (CBC-MAC)
    - Data confidentiality: uses CTR block cipher mode of operation with AES for encryption.

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



References

- Stallings, William. *Network security essentials: applications and standards*. Pearson, 2016.
- The Internet Society. (2004). *Extensible Authentication Protocol* (*EAP*) (RFC 3748). Internet Engineering Task Force (IETF). https://www.ietf.org/rfc/rfc3748.txt
- Nikander, Pekka. (2002). Authorization and charging in public WLANs using FreeBSD and 802.1x. 109-119.
- Hewlett Packard Enterprise Development LP. (s.d.). Packet formats. https://support.hpe.com/techhub/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485048061.htm
- *Reti di Calcolatori - Protocolli data link layer per Wireless LAN*. Università degli Studi di Napoli Federico II. http://wpage.unina.it/fpalmier/Reti/Datalink%20WLAN.pdf