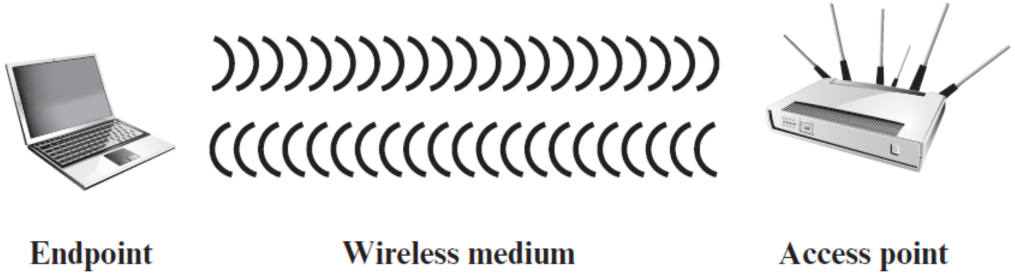
# Wireless Network Security

Dr. Mana Khatua
Assistant Professor
Dept. of CSE, IIT Guwahati
Email: manaskhatua@iitg.ac.in

# Wireless Security Overview

- Security requirements for wireless are the same with wired environment.
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability

- Key Factors Contributing to Risks
  - Channel: broadcast communication; **more susceptible** to eavesdropping and jamming
  - Mobility: contributes **additional risks**
  - Resources: advanced OS, but **limited resources** (memory, processing)
  - Accessibility: Certain devices (sensors, robots) may be **left unattended** for long time



# Wireless Network Threats

- Accidental association
- Malicious association
- Ad hoc networks — Lack of central point of control
- Non-traditional networks — e.g. Bluetooth, Barcode reader, Handhold PDAs
- Identity theft (MAC spoofing)
- Man-in-the-Middle attacks
- Denial of service (DoS)
- Network injection — Bogus reconfiguration commands to routers /switches exposed to nonfiltered traffic

# Wireless Security Measures

wireless security measures dealing with **three components** -

- ❑ Securing wireless transmission
  - Signal hiding technique (for hiding wireless AP)
    - Turn off SSID broadcasting by AP
    - Assign cryptic name to SSID
    - Reduce signal strengths
    - Directional antennas
  - Encryption of wireless transmission

- ❑ Securing wireless access point (AP)
  - Access control policy
    - it is typically based on the identity of the user who requests access to a resource
  - Authentication mechanism
    - to make sure the identity is who they say they are.


- ❑ Securing wireless networks
  - Enable anti-virus, anti-spyware, firewall
  - Turn off SSID broadcasting by routers
  - Change default identifier on router
  - Change router’s pre-set password
  - Apply MAC-filtering
  - Use encryption for traffic

# IEEE 802.11 Wireless LAN

- IEEE 802 committee responsible for LANs
- In 1990, IEEE 802.11 WG was formed

**Aims:**

- To develop a protocol & transmission specifications for Wireless LAN
- **Developed IEEE 802.11i WLAN Security Specification**

- The Wi-Fi alliance formed in 1999. This is an industry consortium.

✓ First standard became popular is 802.11b in 1999

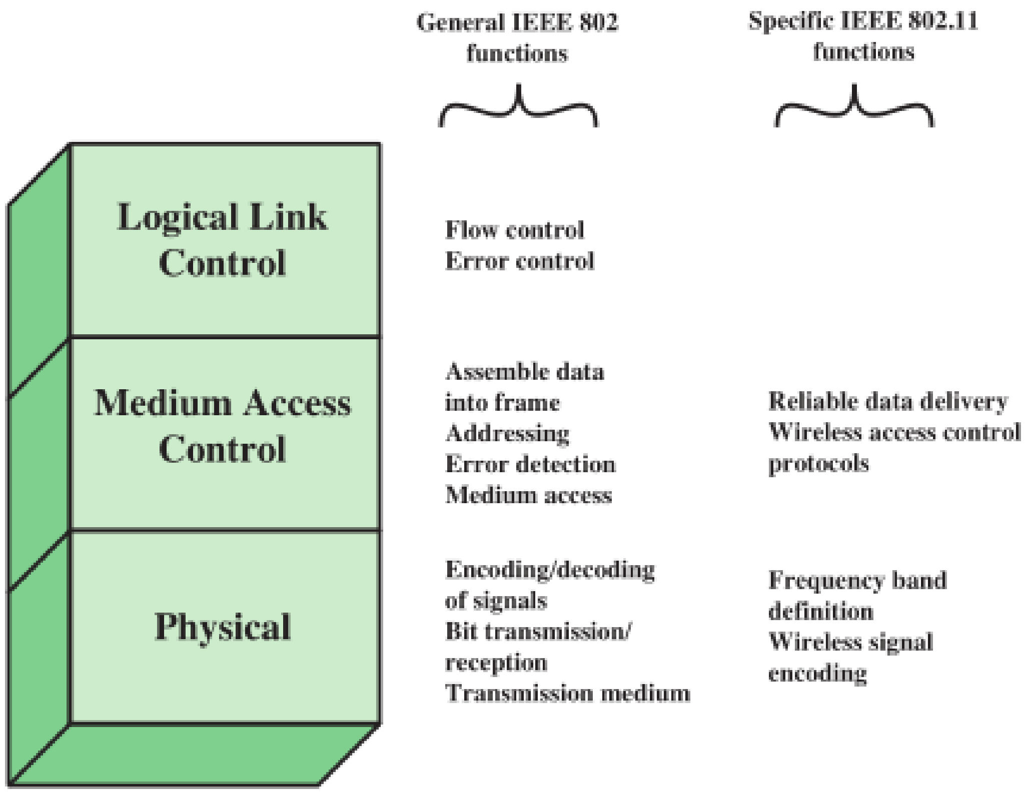
✓ Developed a certification procedure for 802.11 security standards
  - ❖ Wi-Fi Protected Access (WPA)
  - ❖ Recent version in WPA2 – it incorporates all features of 802.11i spec

# IEEE 802.11 Protocol Stack

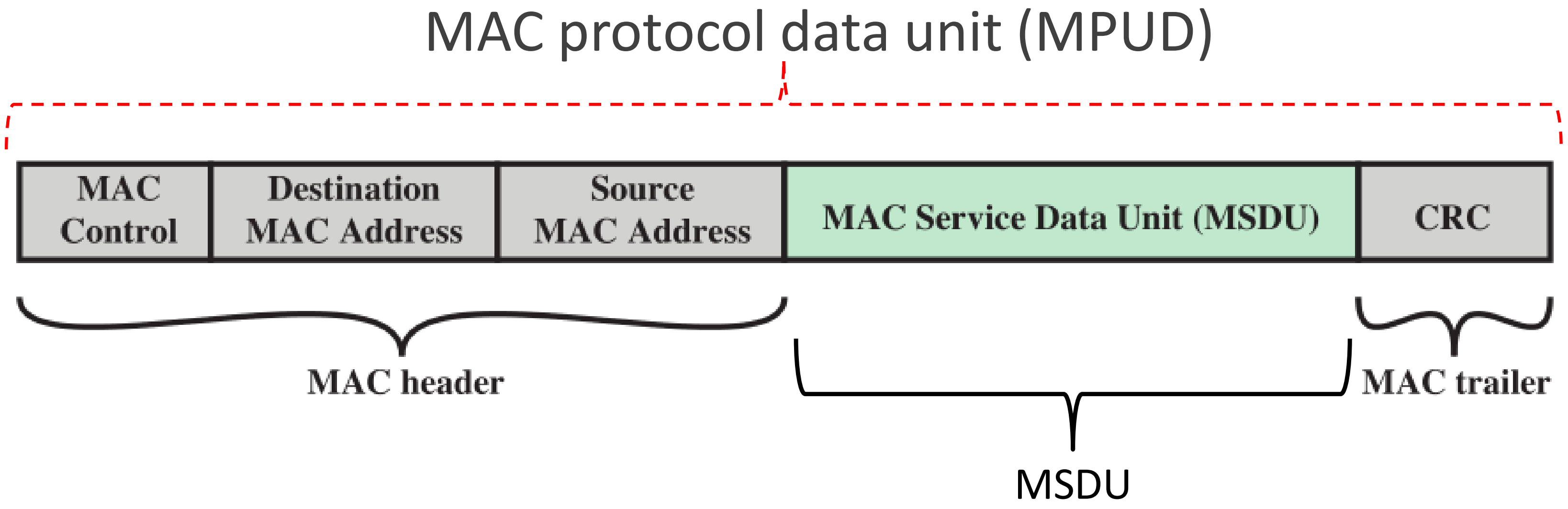
**LLC**:
- keeps track of frame transmissions
- handle frame retransmissions

**MAC layer**
- Addressing
- MAC framing from data
- Medium Access

**Physical layer**
- encode/decode signals
- Bit transmission/reception
- Transmission medium



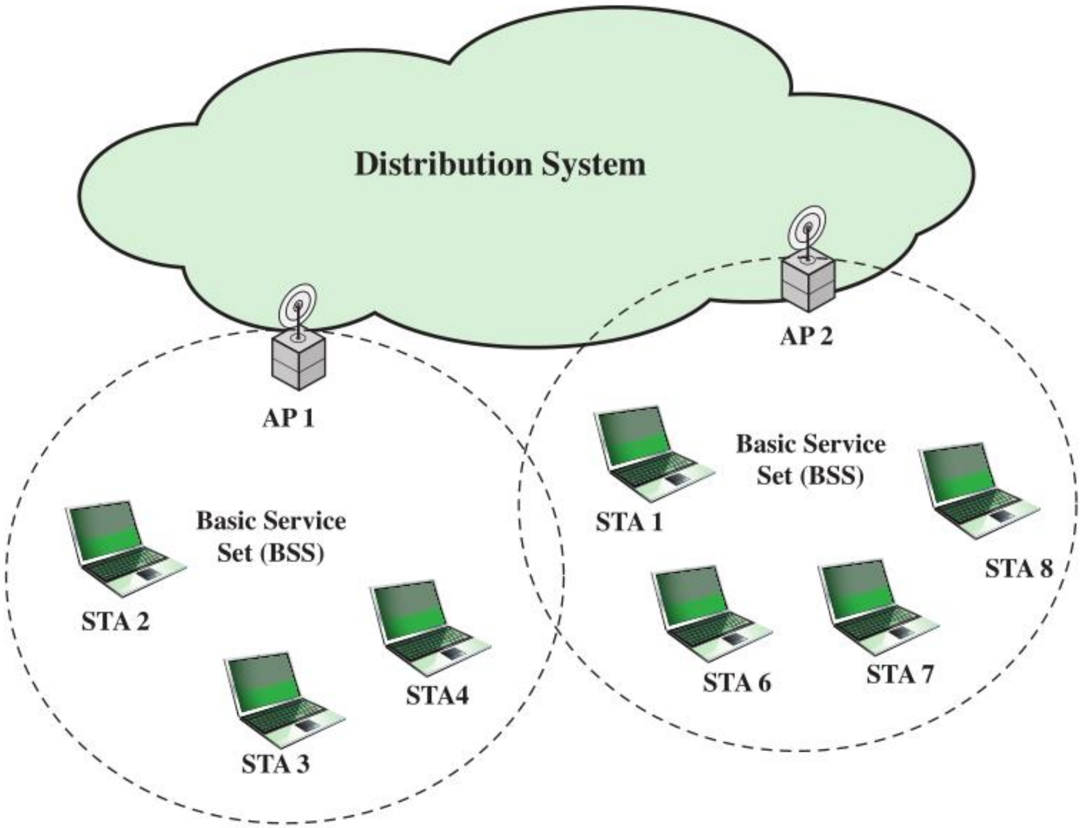
# MAC Frame (MPUD)




CRC: Cyclic Redundancy Check. Also known as Frame Check Sequence (FCS).

This is an error-detecting code, such as that which is used in other data-link control protocols.

# IEEE 802.11 BSS, ESS




BSS (basic service set): the smallest building block.

BSS consists of a set of stations controlled by a single coordination function.

BSSs connected via APs. APs functions as bridges.

ESS: two or more BSSs are connected via Distribution System (DS)

IBSS (independent BSS): When all stations in the BSS are mobile stations that communicate directly with one another (not using an AP)

# IEEE 802.11 Services

| Service | Provider | Used to support |
|---|---|---|
| Association | Distribution system | MSDU delivery |
| Disassociation | Distribution system | MSDU delivery |
| Re-association | Distribution system | MSDU delivery |
| Authentication | Station | LAN access and security |
| De-authentication | Station | LAN access and security |
| Distribution | Distribution system | MSDU delivery |
| Integration | Distribution system | MSDU delivery |
| MSDU delivery | Station | MSDU delivery |
| Privacy | Station | LAN access and security |

**Re-association:** Enables an established association to be transferred from one AP to another
**Distribution**: when the MPDUs must traverse the DS to get destination STA
**Integration**: transfer of data between a STA on an 802.11 LAN and a STA on an 802.x LAN.

# Wireless LAN Security Protocols

- Wired Equivalent Privacy (WEP) algorithm
  - 802.11 privacy by 802.11 work group

The original native security mechanism for WLAN.

- Used to protect wireless communication from eavesdropping (confidentiality)
- Prevent unauthorized access to a wireless network (access control)
- Prevent tampering with transmitted messages (integrity)
- Provide users with the equivalent level of privacy inbuilt in wireless networks (User's role)

**Disadvantage**: very week w.r.t. security & privacy

802.11 Task Group **i** is formed to address the issue.

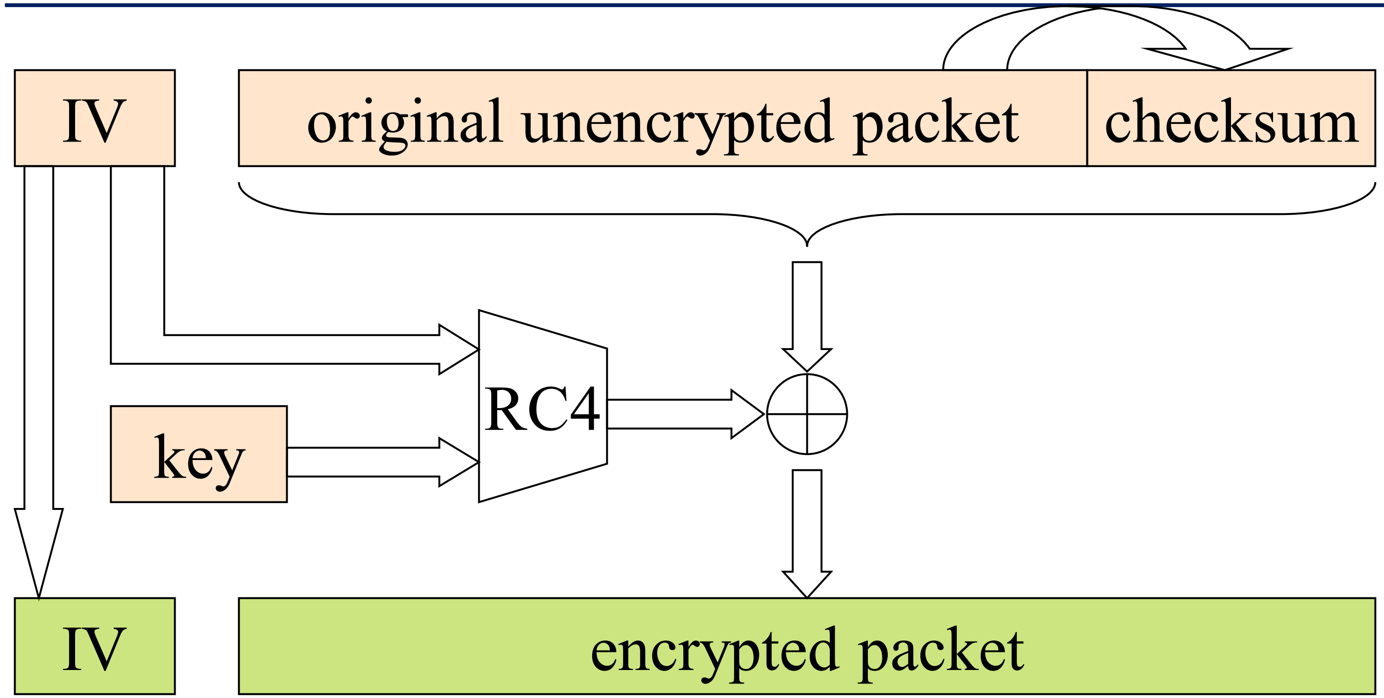
- Wi-Fi Protected Access (WPA)
  - eliminates most of the 802.11 security issues
  - it was based on the current state of the 802.11i standard

Final form of the standard

- Robust Security Network (RSN)

- Wi-Fi Protected Access 2 (WPA2)

# How WEP Works




- IV (initialization vector)
  - There are $2^{24}$ different IVs
- RC4 is an Encryption Algorithm

- **WEP Flaws and Vulnerabilities**
  - Weak keys for encryption
  - IV reuse and small size

# Wi-Fi Protected Access (WPA)

- New security technique WPA in the year 2002-03
- Replacement of security flaws in WEP
- Improved data encryption
- Strong user authentication
- Because of many attacks related to static key, WPA minimize shared secret key in accordance with the frame transmission
- Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data.

# WPA2

- ✓Based on the IEEE 802.i standard
- ✓The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- ✓The encryption in WPA2 is done by utilizing either AES or TKIP (Temporal Key Integrity Protocol)

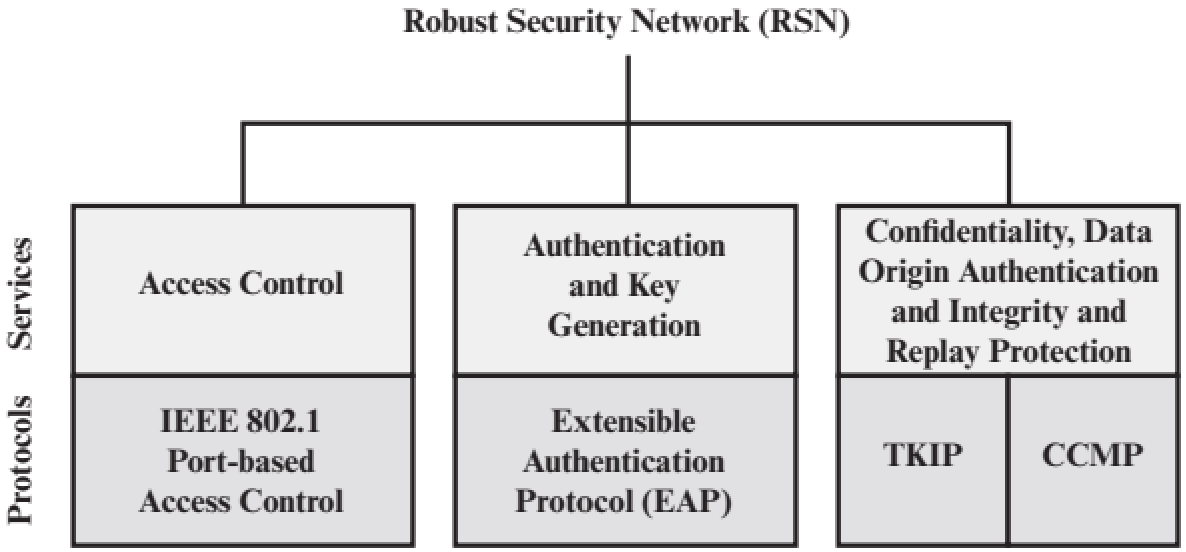
- ✓2 versions: Personal & Enterprise
- ✓The Personal mode uses a PSK (Pre-shared key) & does not require a separate authentication of users
- ✓The enterprise mode requires the users to be separately authenticated by using EAP (Extensible Authentication Protocol)

- ✓WPA3 has been proposed, not used extensively till now.

# WEP vs WPA vs WPA2

| | WEP | WPA | WPA2 |
|---|---|---|---|
| **Year introduced** | 1999 | 2003 | 2004 |
| **Encryption protocol** | Fixed-key | TKIP (Temporal Key Integrity Protocol) | CCMP (Counter Mode CBC-MAC Protocol) |
| **Session key size** | 64-bit/128-bit | 256-bit | 256-bit |
| **Cipher type** | RC4 stream cipher | TKIP (RC4-based) | AES |
| **Data integrity** | Cyclic Redundancy Check | Message Integrity Check | CCMP |
| **Authentication method** | Open system /Shared key | Pre-Shared Key (PSK) | PSK + PMK (Pairwise Master Key) |
| **Key management** | Symmetric key encryption | WPA + WPA-PSK | PMK + PSK |
| **Pros** | Better than no security | i) TKIP encryption<br>ii) 256-bit key for encryption | i) Stronger encryption method: AES<br>ii) Solves prior issues |
| **Cons** | i) Fixed-key encryption<br>ii)many vulnerabilities | Many security vulnerabilities still exist | Require more processing power |

# Services in RSN



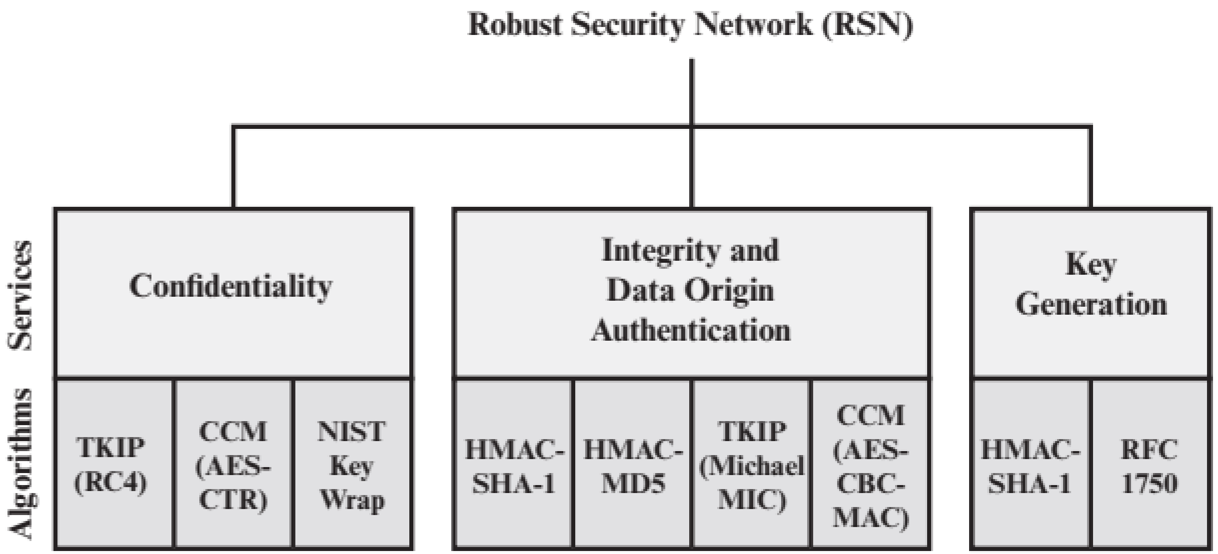

Latest Security Standard by IEEE 802.11 Task Group I

Access Control (as Security Function) – It works with any authentication protocol and key exchange

Authentication – It is mutual authentication. Also do secret key exchange for secured communication

Privacy with message integrity – MAC-level data encryption and message integrity code (MIC) are used to ensure confidentiality, integrity, origin authentication, etc.

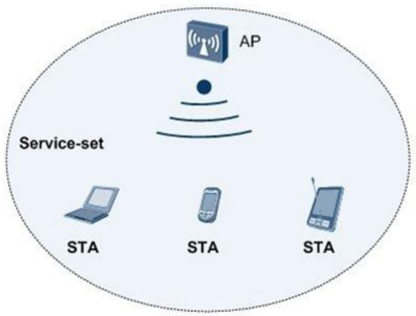
# Cryptographic Algorithms in RSN



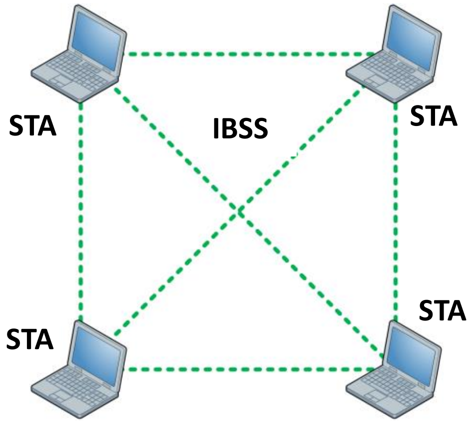

(b) Cryptographic algorithms

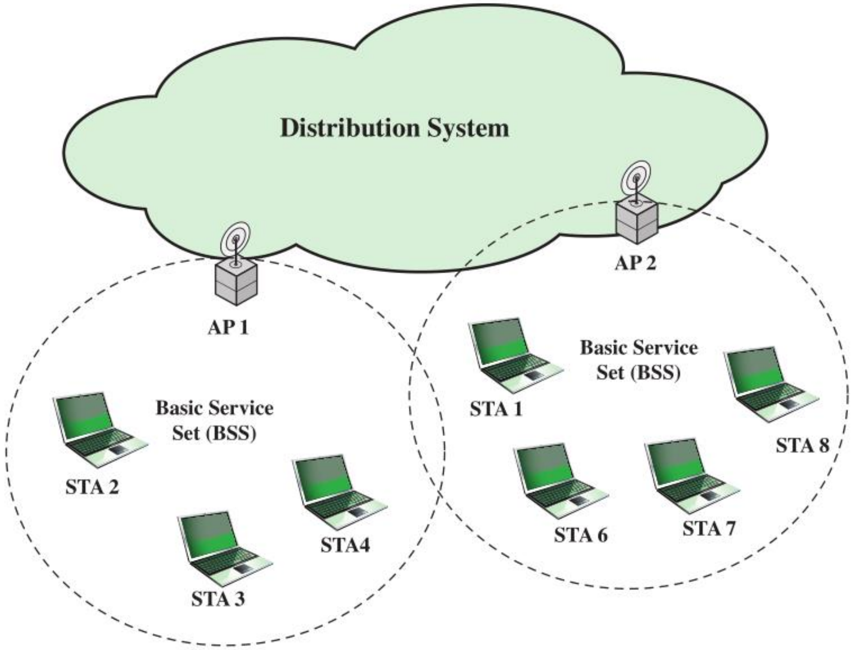
| | | |
|---|---|---|
| CBC-MAC | = | Cipher Block Chaining Message Authentication Code (MAC) |
| CCM | = | Counter Mode with Cipher Block Chaining Message Authentication Code |
| CCMP | = | Counter Mode with Cipher Block Chaining MAC Protocol |
| TKIP | = | Temporal Key Integrity Protocol |

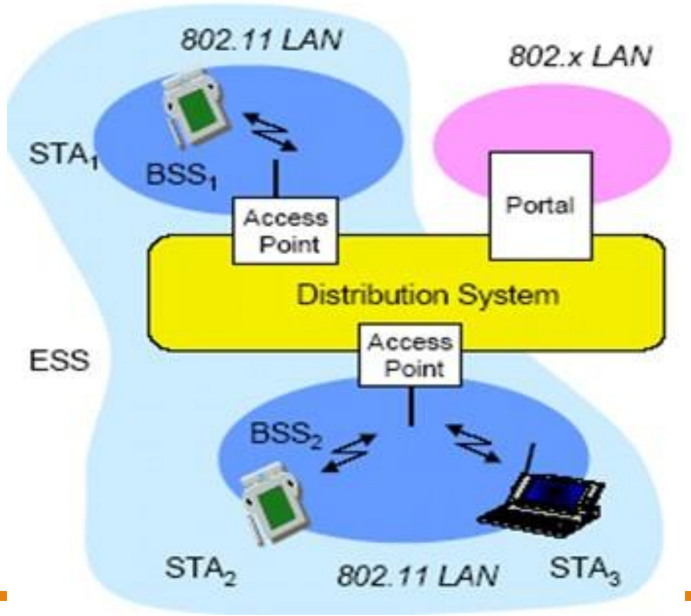
# Types of Configuration



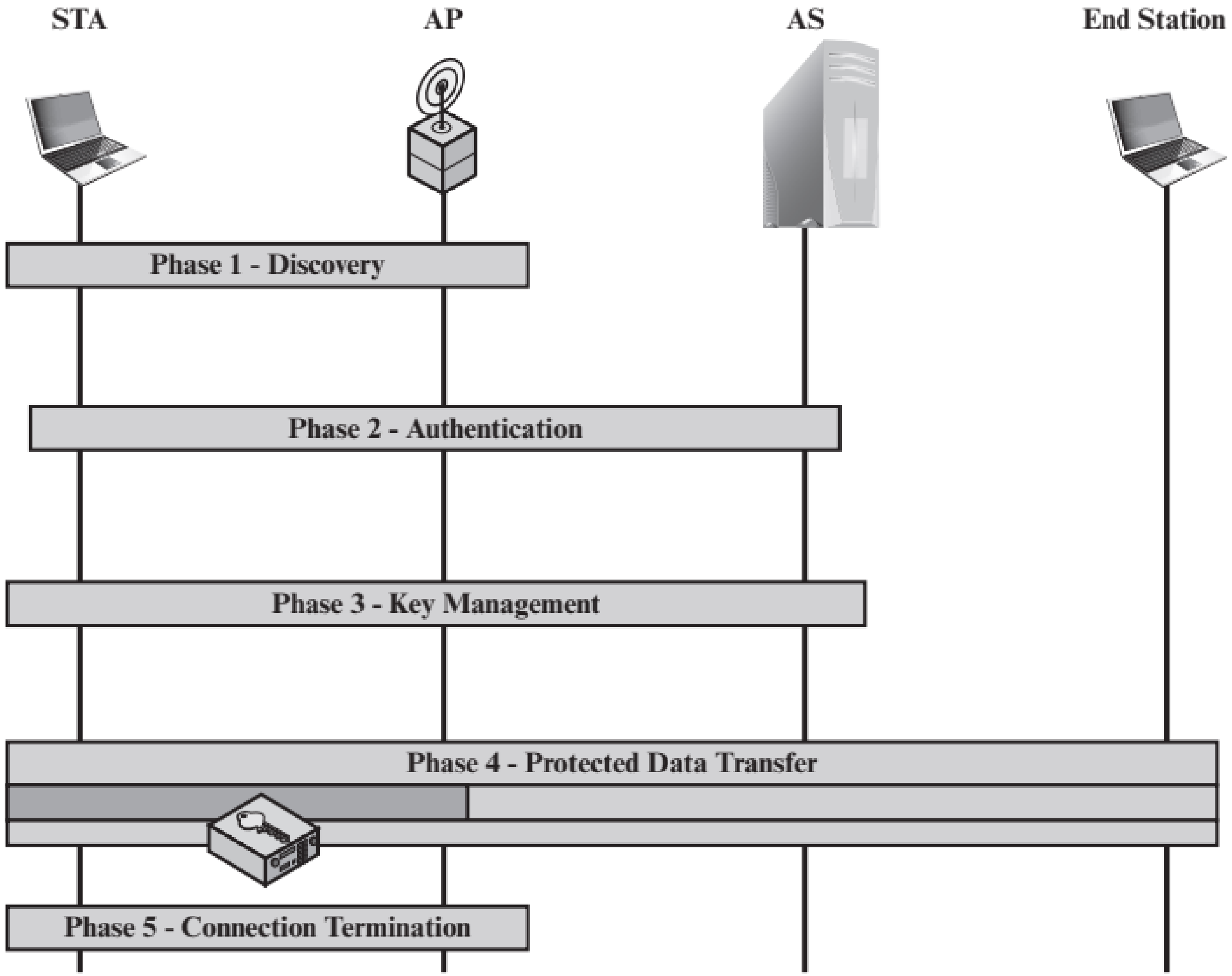

- 802.11i security is limited to BSS
- End-to-end security is provided by upper layer



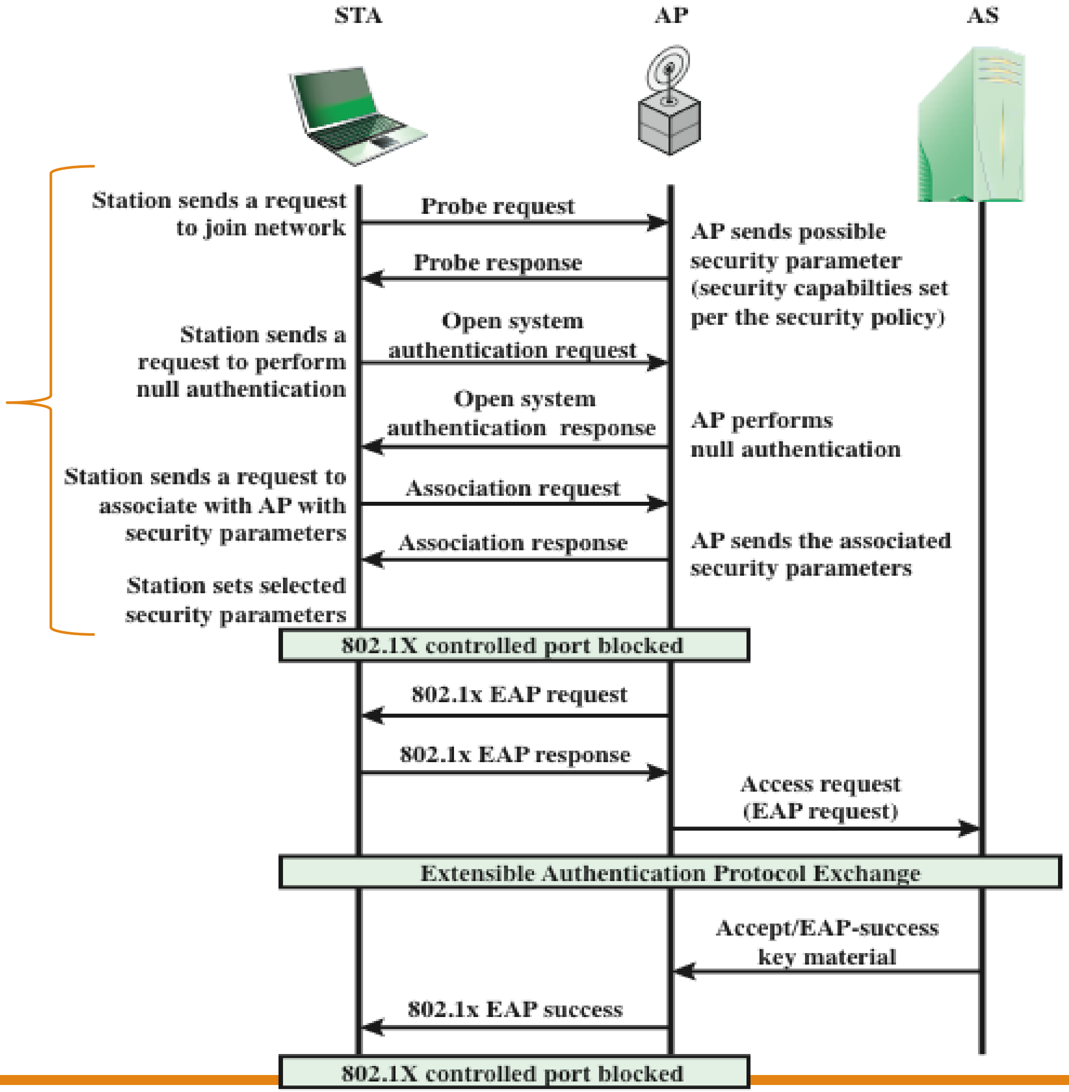



# 802.11i Phases of Operations



# (1) Discovery Phase




**Purpose of Discovery Phase:**

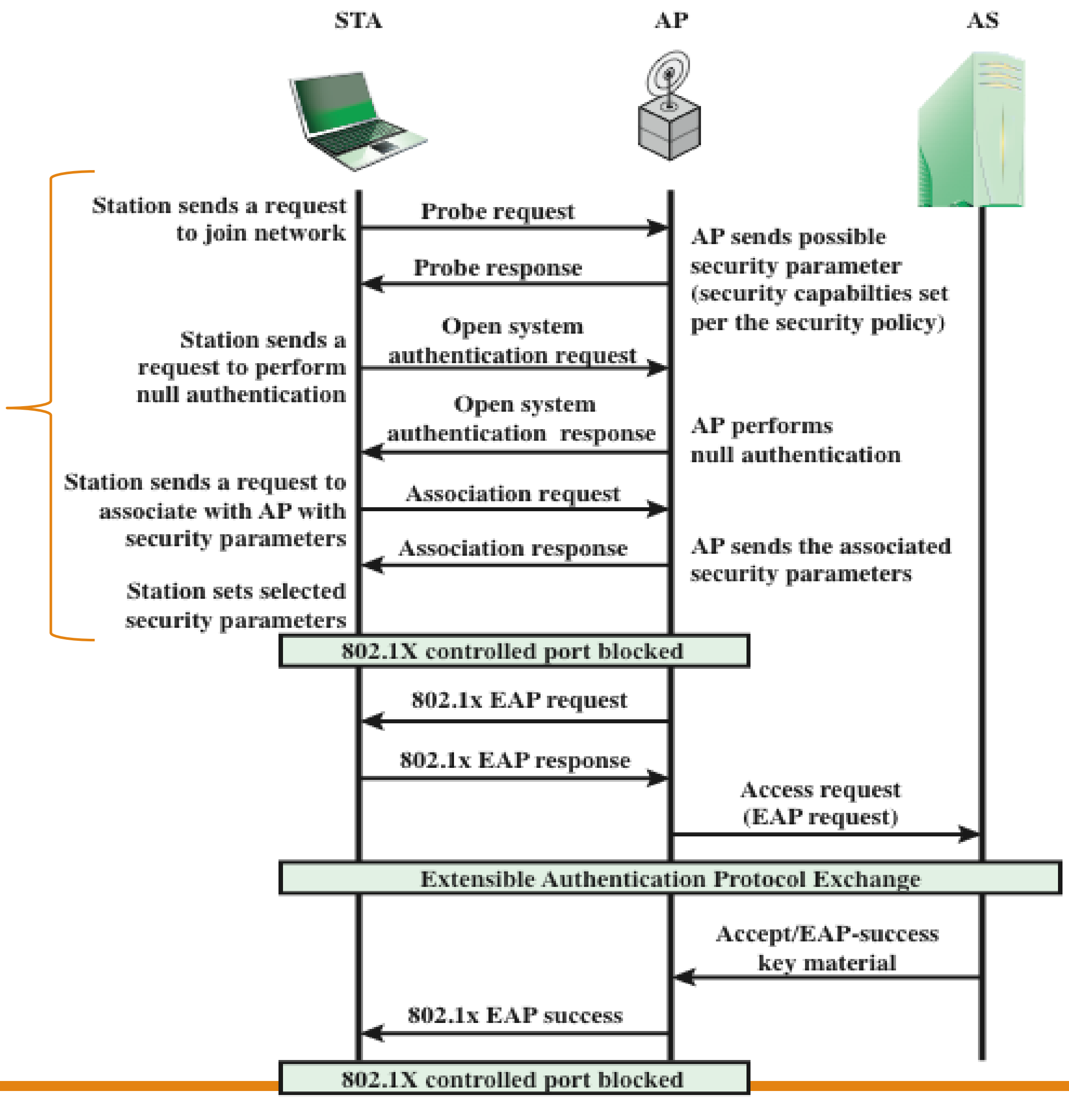
For an STA and an AP

- ✓ to recognize each other,
- ✓ agree on a set of security capabilities,
- ✓ establish an association for future communications

**Security Capabilities:**

- ✓ Confidentiality & Integrity protocols (**Cipher suite**)
  - ➢ TKIP
  - ➢ CCMP
  - ➢ Vendor specific
- ✓ Authentication & Kay management approach (**AKM suite**)
  - ➢ IEEE 802.11X (Port based network access control)
  - ➢ Vendor specific

# Discovery Phase




**Discovery Procedure:**

AP uses
- Beacon & Probe Response to advertise its 802.11i security policy

STA uses the above messages
- to identify an AP
- to associate with the AP

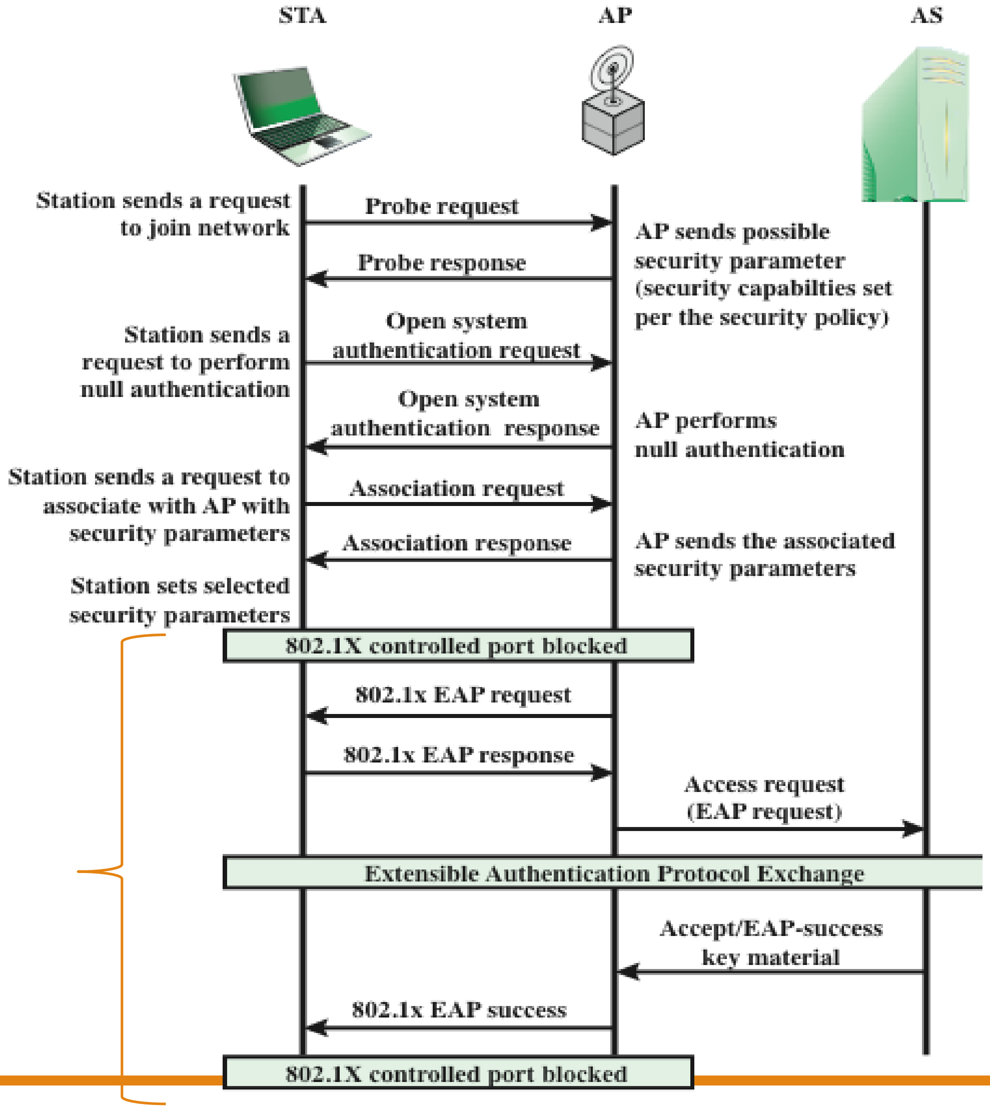
Open system authentication
- Only to maintain backward compatibility with the IEEE 802.11 state machine
- STA & AP simply exchanges IDs

Association
- STA & AP agree on a set of security capabilities to be used.
- Using Association Request, STA informs its selection from the set declared by AP (using Beacon / Probe Response)

AP can refuse association request

STA also can block rogue AP

# (2) Authentication Phase

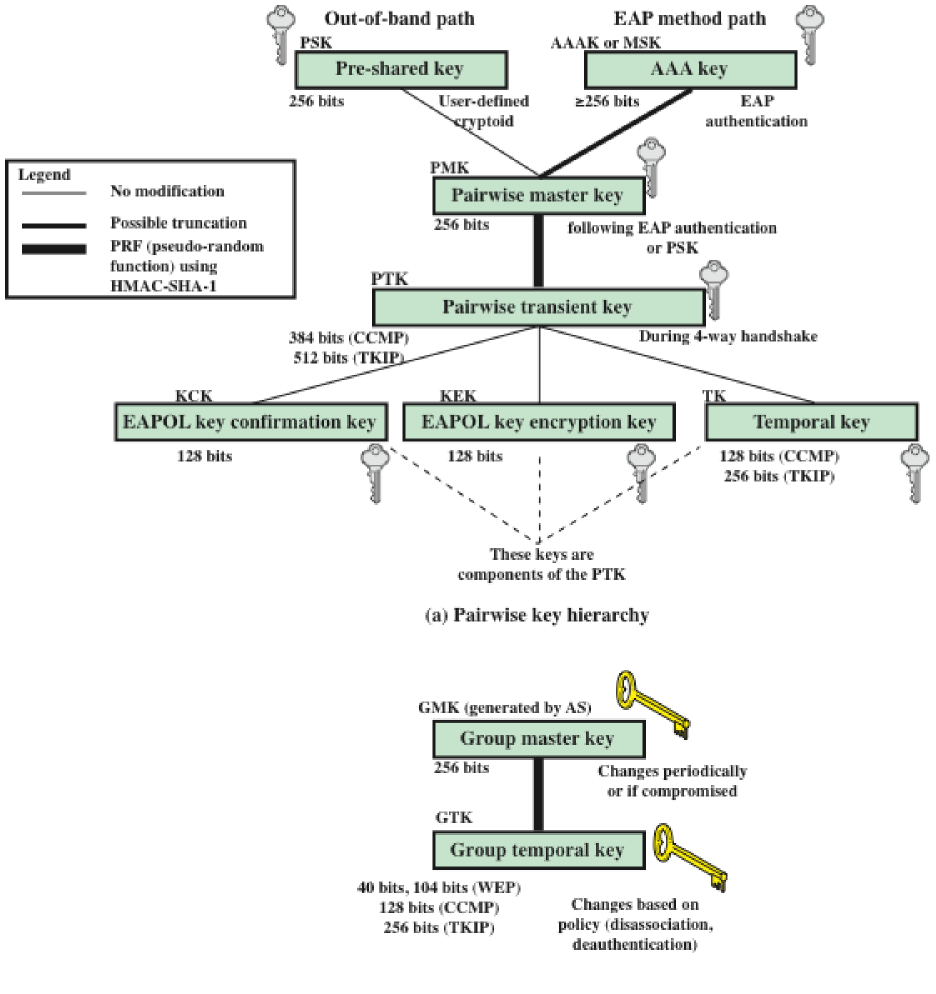



This is mutual authentication
- Between STA & AS located in a DS

IEEE 802.11i makes use of IEEE 802.11X Port-based Network Access Control
- Extensible Authentication Protocol (EAP)
  - Supplicant ~STA
  - Authenticator ~AP
  - Authentication server (AS)

**Consists of three steps:**
- Connect to AS
  - By request-Response, AP → STA → AS
- EAP exchange
  - authenticates the STA and AS to each other
  - STA-to-AP message flow uses EAP over LAN (EAPOL) protocol,
  - AP-to-AS message flow uses Remote Authentication Dial In User Service (RADIUS) protocol
- Secure key delivery
  - the AS generates a master session key (MSK)
  - sends it to the STA secretly

# (3) Key Management Phase




(a) Pairwise key hierarchy

(b) Group key hierarchy

In this phase, a variety of cryptographic keys are generate 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.

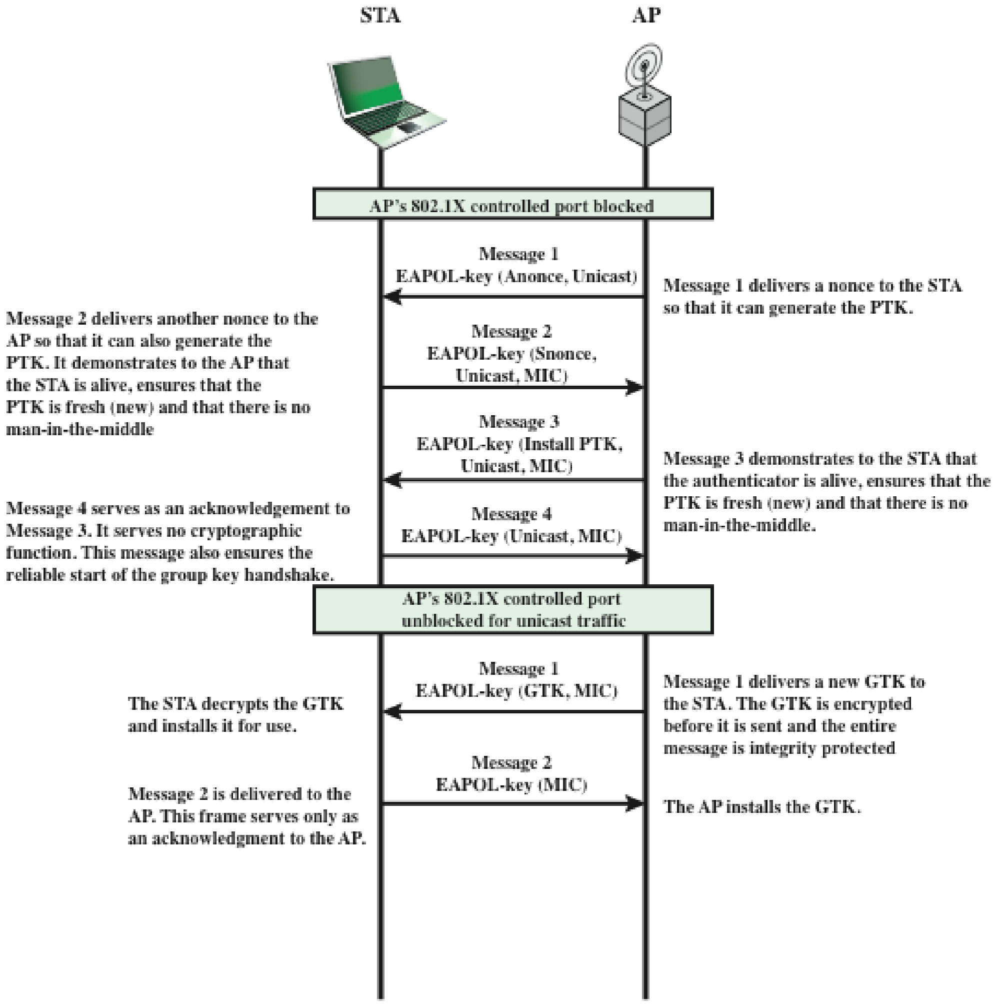
# IEEE 802.11i Keys

| 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)<br>384 (CCMP) | Composite key |
| TK | Temporal Key | Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic. | 256 (TKIP)<br>128 (CCMP) | Traffic key |

# IEEE 802.11i Keys

| Abbreviation | Name | Description / Purpose | Size (bits) | Type |
|---|---|---|---|---|
| GTK | Group Temporal Key | Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic. | 256 (TKIP)<br>128 (CCMP)<br>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 |

# Key Distribution




**4-way handshake:**

The upper part of the Figure shows the MPDU exchange for distributing pairwise keys.

**Group Key Handshake**

the AP generates a GTK and distributes it to each STA in a multicast group.

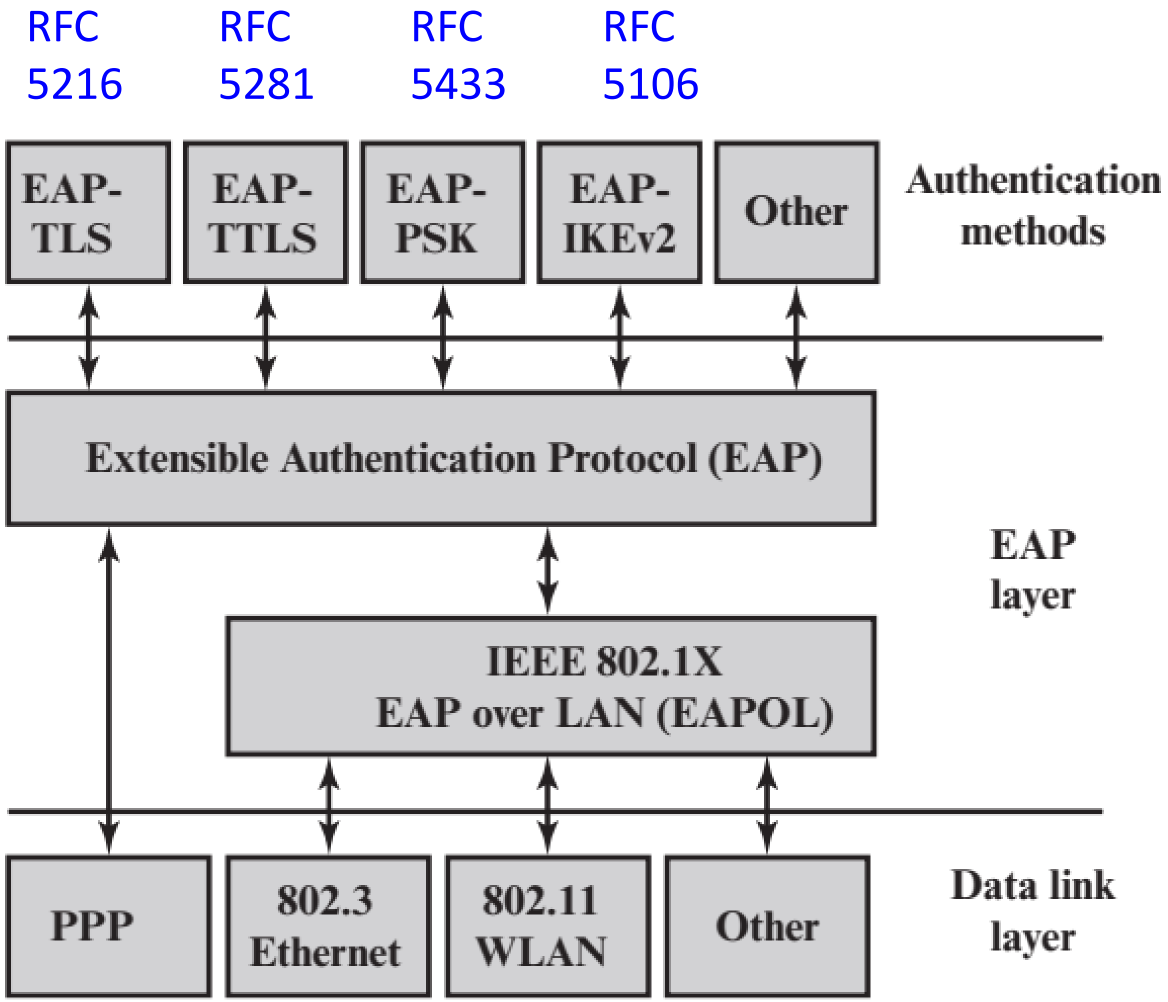
# (4) Protected Data Transfer Phase

IEEE 802.11i defines two schemes for this:

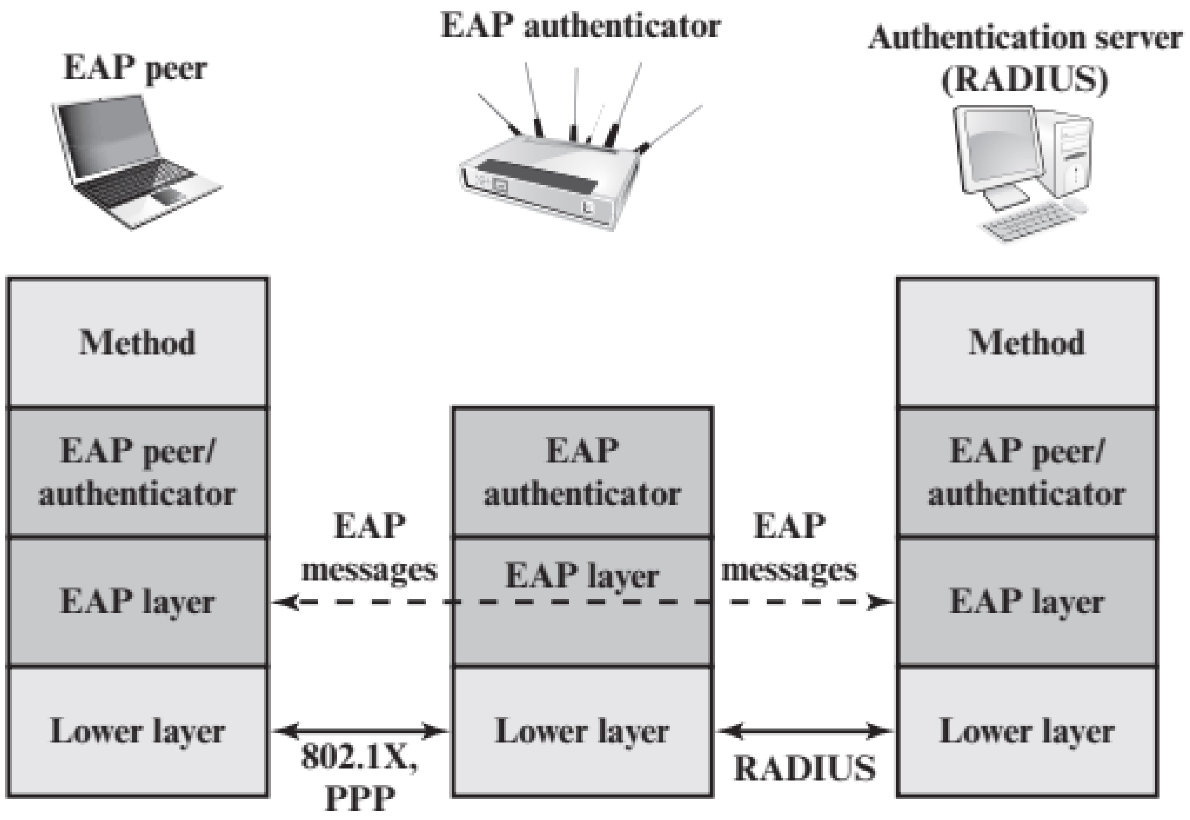
- Temporal Key Integrity Protocol (TKIP) – for older WiFi devices using WEP
- Counter Mode-CBC MAC Protocol (CCMP) – for new WiFi devices using WPA / RSN

- TKIP and CCMP both provides two services:
  - Message integrity
    - In TKIP: using message integrity code (MIC) generated by algorithm Michael
    - In CCMP: using cipher block chaining message authentication code (CBC-MAC)
  - Data confidentiality
    - In TKIP: using RC4 based encryption
    - In CCMP: using AES for encryption

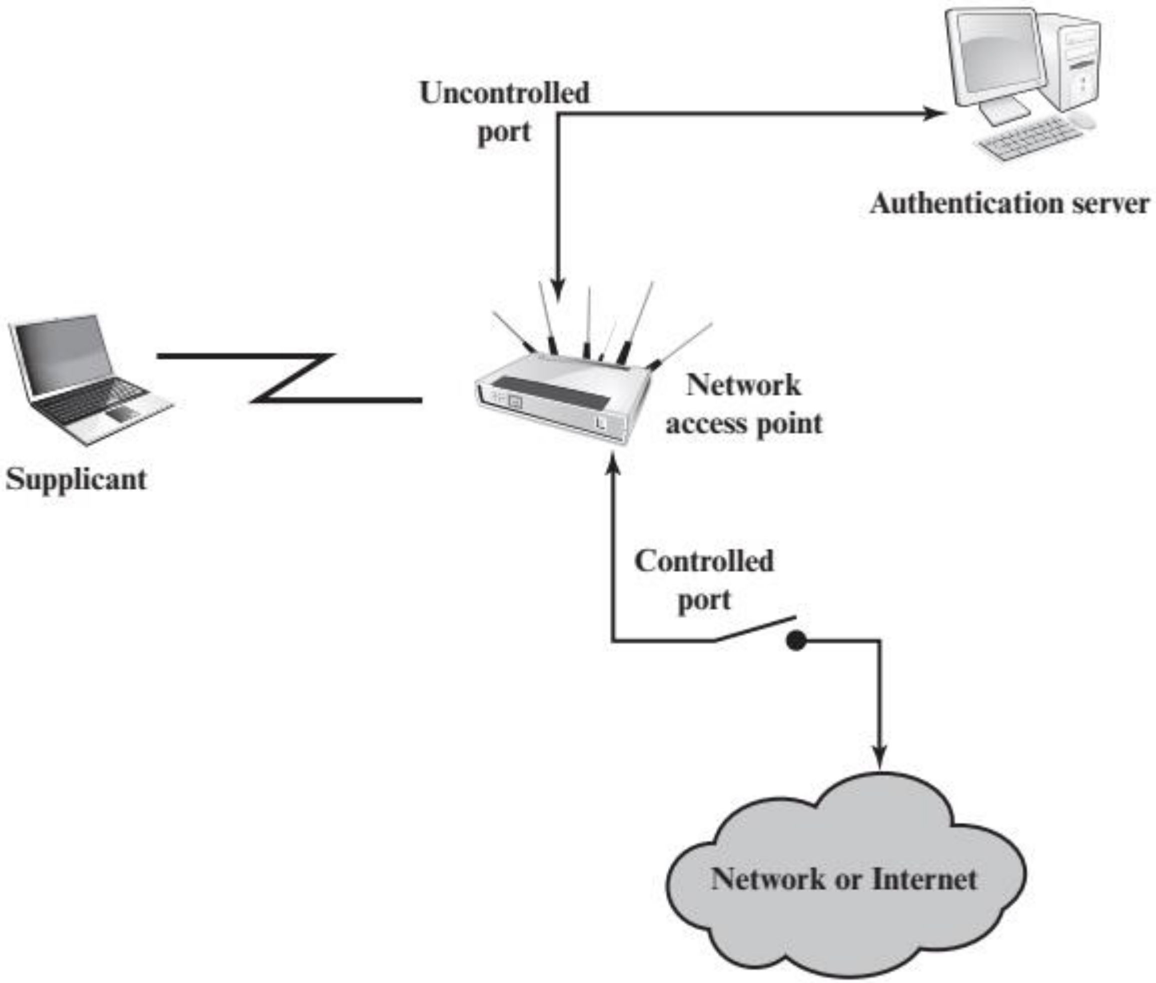
# EAP Layered Context



# EAP Protocol Exchanges



# IEEE 802.1X Access Control




Until the AS authenticates a supplicant (i.e. client), the 802.1X control channel is unblocked, but the 802.11 data channel is **blocked**.

Once a supplicant is authenticated and authorised, the data channel becomes **unblocked**

802.1X uses the concepts of controlled and uncontrolled ports.

Ports are logical entities defined within the authenticator and refer to physical network connections,

Each logical port is mapped to one these two types of physical ports (controlled /uncontrolled)

# Cont

Thank You