4TC - ARM

IEEE 802.11: mobility and evolutions

membre de UNIVERSITÉ DE LYON

Département Télécommunications
Services & Usages

INSA LYON

IEEE 802.11: mobility and evolutions

The plan for today

- IEEE 802.11 network architecture.
- Mobility management.
- Standard evolution.

IEEE 802.11: The beginnings

- In 1985, the US Federal Communications Commission (FCC) created the Industrial, Scientific and Medical band (ISM) for non-licensed applications (2,4GHz).

- In 1990 the IEEE established the 802.11 committee.

- The IEEE 802.11 standard was finalized in 1997 and became the de-facto standard for WLAN.

IEEE 802.11: The beginnings

- IEEE is just a standardization entity – no control over the correct implementation of the standard.

- In 1999, several companies (Cisco, Alcatel-Lucent, Motorola, Nokia …) formed the Wireless Ethernet Compatibility Alliance (WECA) for certification purposes.

- In 2002, WECA was rebranded as the W-Fi alliance, with around 400 members today.

IEEE 802.11: The principles

- A standard that covers both the MAC and PHY layers.

- Build on the success of Ethernet, and enable the creation of Wireless LANs.

- Works both in a pure ad-hoc and infrastructure mode.

- The classical goal of a standard: inter-operability between equipments.

IEEE 802.11: The principles

PHY Layer

- Initial versions use spread spectrum techniques: either DSSS (Direct-Sequence Spread Spectrum) or FHSS (Frequency-Hopping Spread Spectrum).

- DSSS is also used in IEEE 802.11b and g.

- OFDM (Orthogonal Frequency Division Multiplexing) was adopted by the IEEE 802.11a standard.

- Since 2004, all the versions of the standard use OFDM.

IEEE 802.11: The principles

MAC Layer

- Channel access defined by different techniques: DCF (Distributed Coordination Function), PCF (Point Coordination Function), HCF (Hybrid Coordination Function).

- DCF is the only access method actually implemented in Wi-Fi products.

- DCF is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

IEEE 802.11: The principles

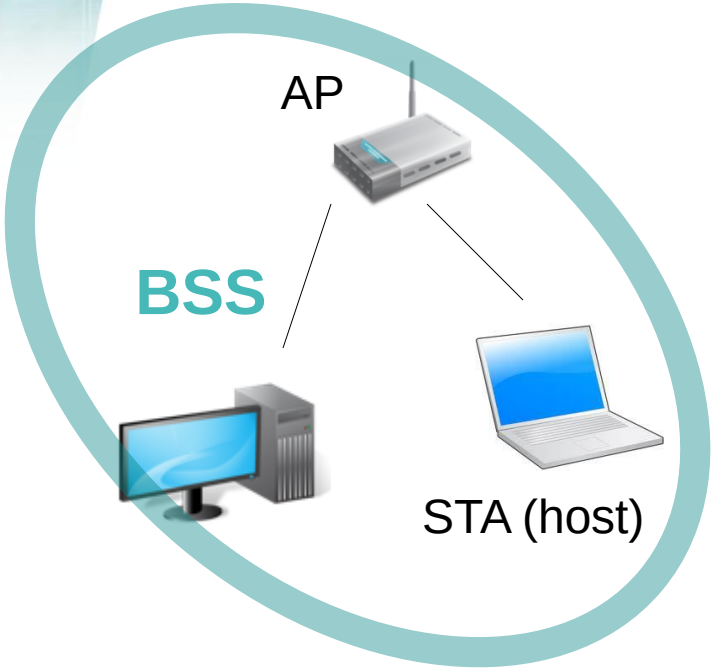
MAC Layer

- Carrier Sense – listen before transmission and back-off if the channel is already used.

- Collision Avoidance – use a larger back-off window (compared with Ethernet) to reduce the probability of successive collisions.

- IEEE 802.11e introduced an evolution of DCF – EDCA (Enhanced Distributed Channel Access), designed for multimedia traffic.

IEEE 802.11: Architecture



Basic Service Set (BSS)

- Formed by an Access Point (AP) and all the associated stations (STA).
- Similar to a “cell” in 2G/3G.
- The BSSID is the MAC address of the AP and is broadcasted periodically.



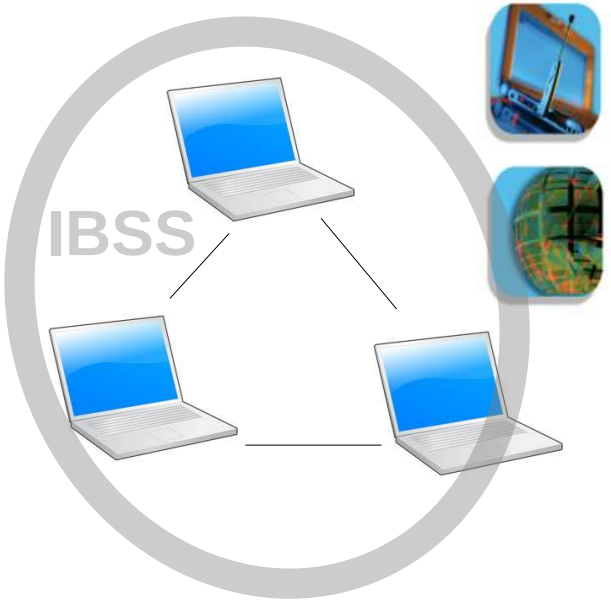
IEEE 802.11: Architecture

Independent Basic Service Set (IBSS)

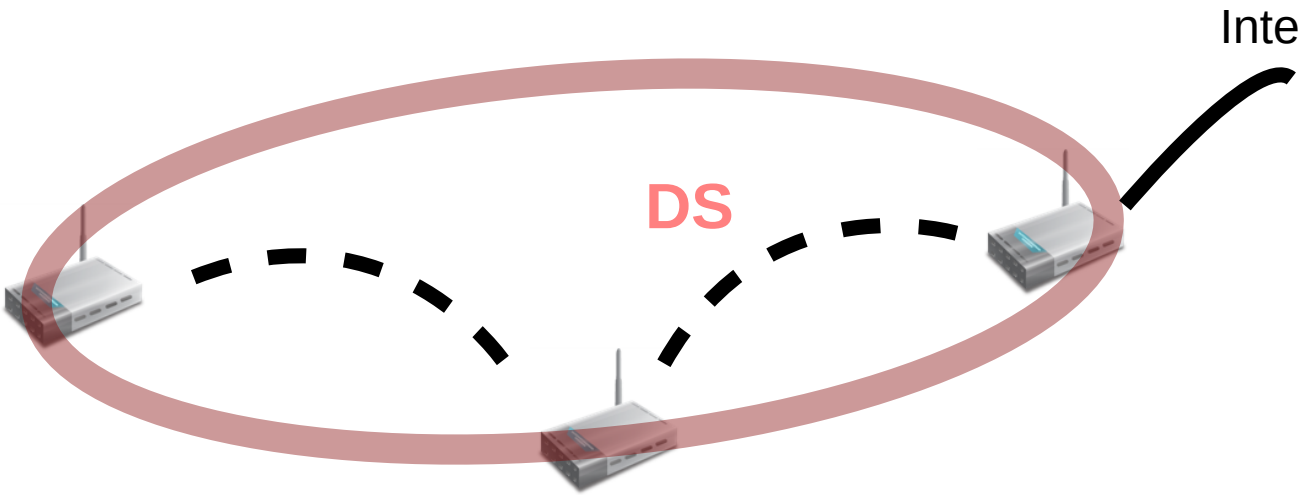
• No AP, only synchronized STAs, one of which acts as a master.

• As close as it gets from ad-hoc networking.

• The BSSID is the MAC address of the master STA and is broadcasted periodically.



IEEE 802.11: Architecture

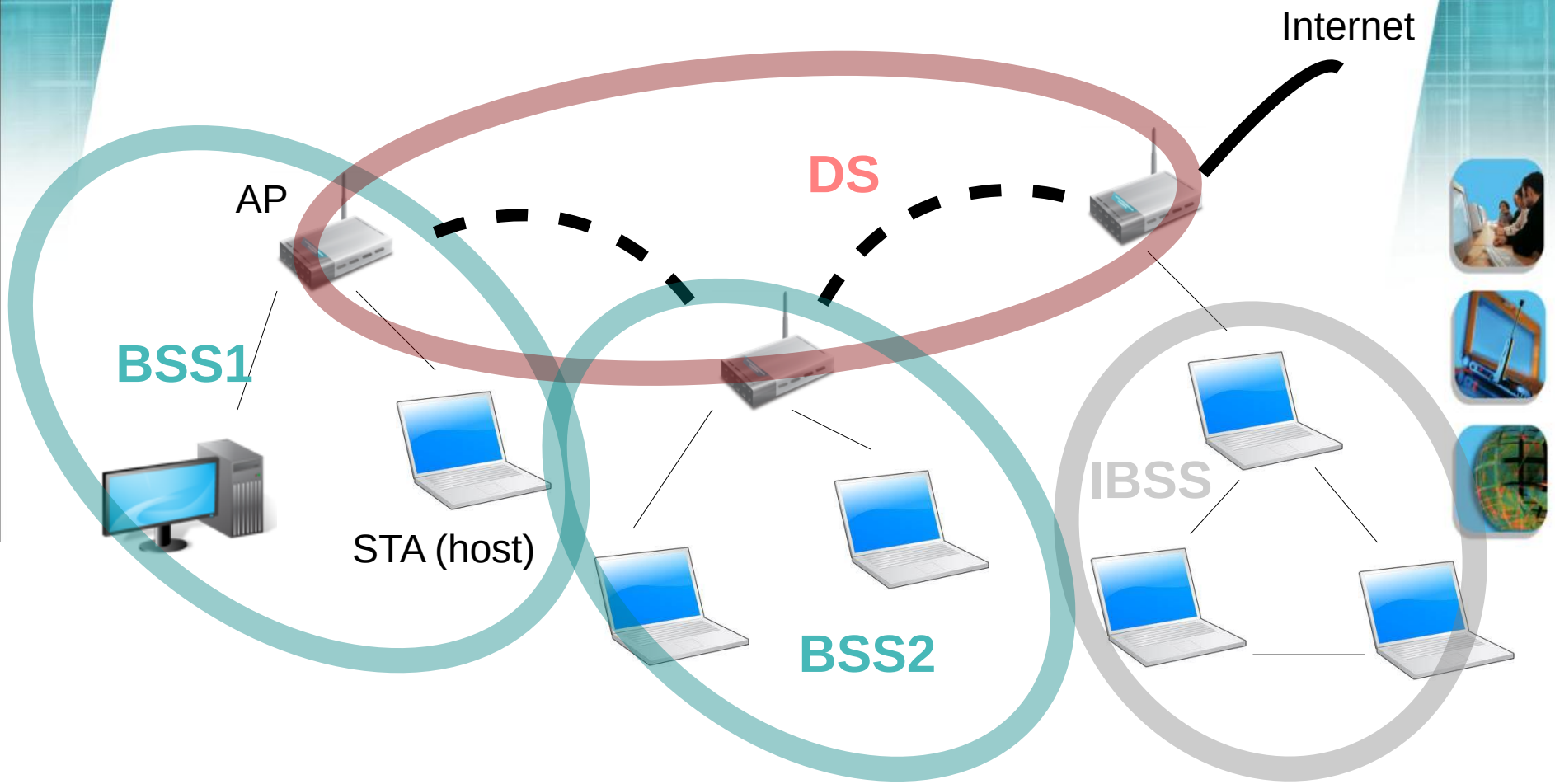


Distribution System (DS)

• A backbone (usually, but not necessarily wired) connecting the APs.

• The DS may use any communication technology, with Ethernet being the most deployed.

IEEE 802.11: Architecture



IEEE 802.11: Architecture

Extended Service Set (ESS)

- An ESS is the union of multiple BSSs connected through a DS.

- The ESS is equivalent to a single IBSS for the logical link control layer.

- The BSSs forming an ESS can use different frequency channels.

- No physical restrictions: BSSs can be collocated, overlapping, or connected through a long range DS.



IEEE 802.11: Mobility

- The usual WiFi user experience – nomadic.

- Mobility is possible in IEEE 802.11 networks.

- The obvious scenario: moving within the area covered by the same AP.

- Handovers between different APs are possible inside an ESS.

IEEE 802.11: Mobility

Parallels with cellular networks

- The DS must implement a location service (not specified by the IEEE 802.11 standard).

IEEE 802.11: Mobility

Parallels with cellular networks

- The DS must implement a location service (not specified by the IEEE 802.11 standard) – similar.

- A STA can be associated with no more than one AP at a given time (hard handover).

IEEE 802.11: Mobility

Parallels with cellular networks

- The DS must implement a location service (not specified by the IEEE 802.11 standard) – similar.

- A STA can be associated with no more than one AP at a given time (hard handover) – similar.

- The STA continuously measures the channel quality for the neighboring APs.



IEEE 802.11: Mobility

Parallels with cellular networks

- The DS must implement a location service (not specified by the IEEE 802.11 standard) – similar.

- A STA can be associated with no more than one AP at a given time (hard handover) – similar.

- The STA continuously measures the channel quality for the neighboring APs – similar.

- The handover is initiated by the STA.



IEEE 802.11: Mobility

Parallels with cellular networks

- The DS must implement a location service (not specified by the IEEE 802.11 standard) – similar.

- A STA can be associated with no more than one AP at a given time (hard handover) – similar.

- The STA continuously measures the channel quality for the neighboring APs – similar.

- The handover is initiated by the STA – different.



IEEE 802.11: Mobility

Network entry

- **Scanning** – STA chooses an AP nearby
  - *Passive*: just wait for the periodic AP beacon
  - *Active*: probe a known AP.

- **Authentication** – STA proves it has legit access to the AP
  - *Open*: this phase is skipped
  - *Secure*: challenge by the AP, the STA needs to know a shared key to answer correctly.

IEEE 802.11: Mobility

Network entry

- **Association** – STA enters the BSS
  - STA -> AP: association request
  - AP -> STA: association reply.



IEEE 802.11: Mobility

Handover

- AP scanning and selection of target AP (by the STA).
- Authentication (if needed) with the target AP.
- Re-association with the target AP.



IEEE 802.11: Mobility

Handover

- AP scanning and selection of target AP (by the STA).
- Authentication (if needed) with the target AP.
- Re-association with the target AP.
- Pair-wise master key (PMK) negotiation – IEEE 802.1X.
- Pair-wise transient key (PTK) negotiation – IEEE 802.11i.
- QoS admission control.



IEEE 802.11: Mobility

IEEE 802.11r amendment (2008)

- Originally, only 4 messages were needed for intra-ESS handover: 2xAuthentication and 2xAssociation.

- Security and QoS admission control highly increased the number of messages and the delay.

- The PTK negotiation needs 4 messages.

- IEEE 802.1X authentication requires a time consuming key negotiation with an authentication server at every handover.



IEEE 802.11: Mobility

IEEE 802.11r amendment (2008)

- Specification of Fast Basic Service Set transitions between APs.

- The PMK is cached in the DS and reused for handovers, avoiding the negotiation process.

- PTK negotiation and QoS admission control are piggybacked with the Authentication and Reassociation messages.



IEEE 802.11: Evolution

- IEEE 802.11 – 2007: groups all the amendments approved between 1997 and 2007
- Definition of different PHY layers: 802.11a/b/g.
- Quality of Service enhancements: 802.11e.
- Security mechanisms: 802.11i.
- Support for specific country regulations: 802.11d/j.
- Interference management in the 5GHz band: 802.11h.



IEEE 802.11: Evolution

- IEEE 802.11 – 2012: includes all the amendments approved between 2007 and 2012
- Multiple antennas and frame aggregation: 802.11n.
- Mobility management: 802.11r/k (AP selection).
- Enhanced security: 802.11w.
- Network management: 802.11v.
- Interworking with external networks: 802.11u.



IEEE 802.11: Evolution

- IEEE 802.11 – 2012: includes all the amendments approved between 2007 and 2012
- Functioning in the 3.7GHz band: 802.11y.
- Mesh networks: 802.11s.
- Vehicular environment: 802.11p.
- Direct communication inside a BSS: 802.11z.



IEEE 802.11: Evolution

• 802.11aa: MAC enhancements for robust video streaming, while maintaining coexistence with other types of traffic.

• 802.11ae: management frames prioritization using existing MAC mechanisms.

IEEE 802.11: Evolution

Active working groups:

• 802.11ac: very high-throughput WLAN in the 5GHz band (wider channel bandwidth, more complex modulations, multi-user MIMO.

• 802.11ad: PHY and MAC operation in the 60GHz band; fast session transfer between 802.11 PHYs.

• 802.11af: PHY and MAC operation on the TV White Space.



IEEE 802.11: Evolution

Active working groups:

- 802.11ah: functioning in sub 1GHz frequencies for long range applications such as smart metering.

- 802.11ai: fast link setup, reduction of association time.

- 802.11aj: very high throughput in the China milimetre-wave bands.

- 802.11ak: bridging mechanisms across 802.11 links.

- 802.11aq: pre-association discovery of services.