UNIVERSITY OF TRENTO
Department of Information Engineering and Computer Science

Wireless Mesh and Vehicular Networks

802.11MAC Fundamentals

Renato Lo Cigno

ANS Group – locigno@disi.unitn.it

http://disi.unitn.it/locigno/teaching-duties/wmvn

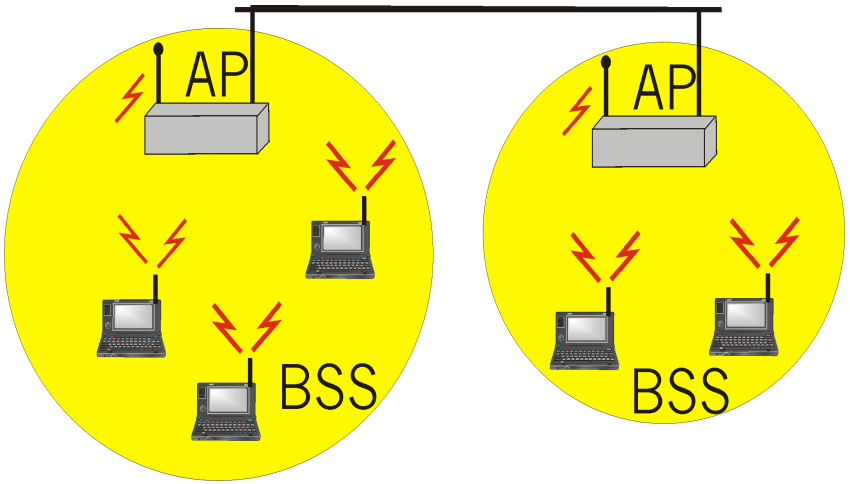
IEEE 802.11

- Wireless LAN standard specifying a wireless interface between a client and a base station (or access point), as well as between wireless clients
- Defines the PHY and MAC layer (LLC layer defined in 802.2)
- Physical Media: radio or diffused infrared (not used)
- Standardization process begun in 1990 and is still going on (1st release ’97, 2nd release ’99, then ’03, ’05, ... ‘12)

- BSS (Basic Service Set): set of nodes using the same coordination function to access the channel
- BSA (Basic Service Area): spatial area covered by a BSS (WLAN cell)
- BSS configuration mode
  - ad hoc mode
  - with infrastructure: the BSS is connected to a fixed infrastructure through a centralized controller, the so-called Access Point (AP)

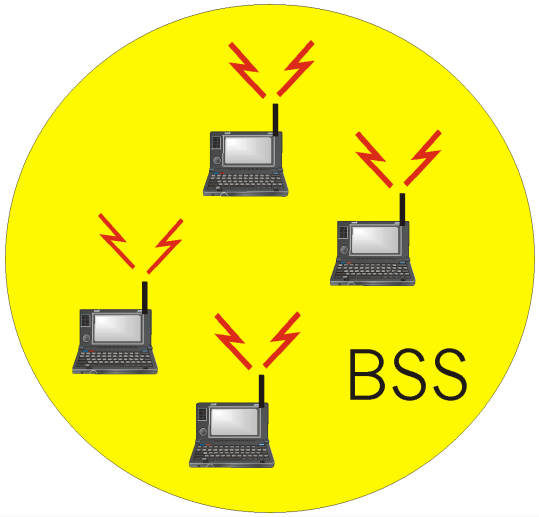
WLAN with Infrastructure

- BSS contains:
  - wireless hosts
  - access point (AP): base station
- BSS's interconnected by distribution system (DS)



Ad Hoc WLANs

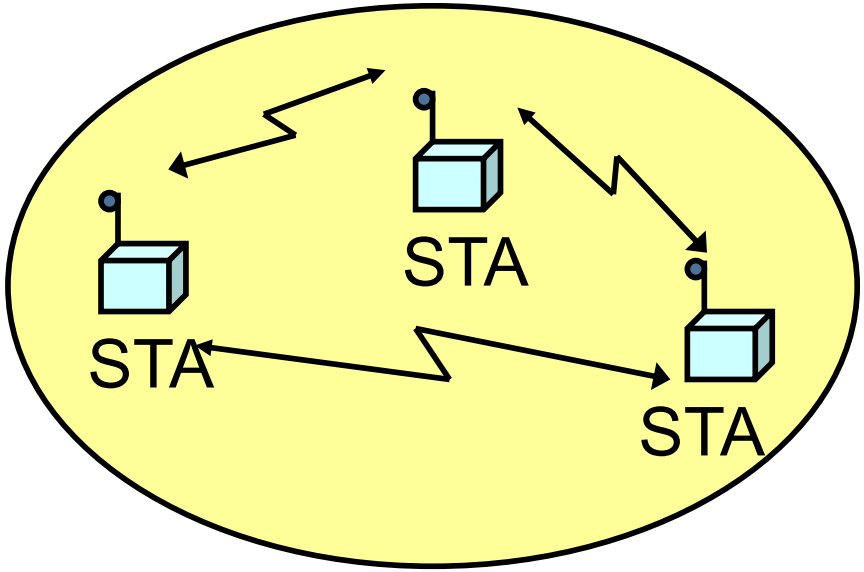
- Ad hoc network: IEEE 802.11 stations can dynamically form a network *without* AP and communicate directly with each other: IBSS Independent BSS
- Applications:
  - Vehicular Networks
  - Meeting in conference room
  - Interconnection of “personal” devices
  - Battlefield
  - ….
- IETF MANET (Mobile Ad hoc Networks) working group; VANET; V2V; V2X; ...



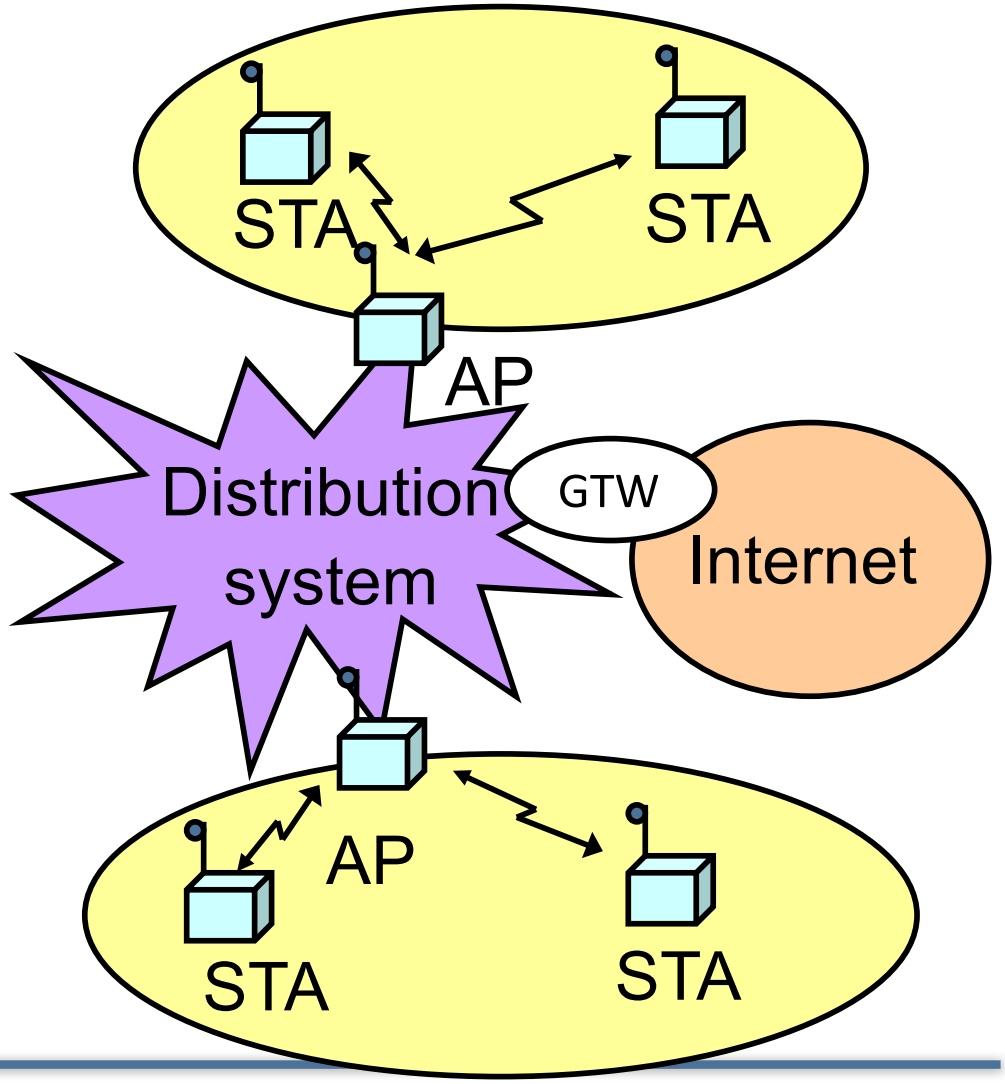
Extended Service Set (ESS)

- Several BSSs interconnected with each other at the MAC layer
- The backbone interconnecting the BSS APs (Distribution System) can be a:
  - LAN (802 family)
  - wired MAN
  - IEEE 802.11 WLAN, possibly meshed (a large part of our course)
- An ESS can give access to the fixed Internet network through a gateway node

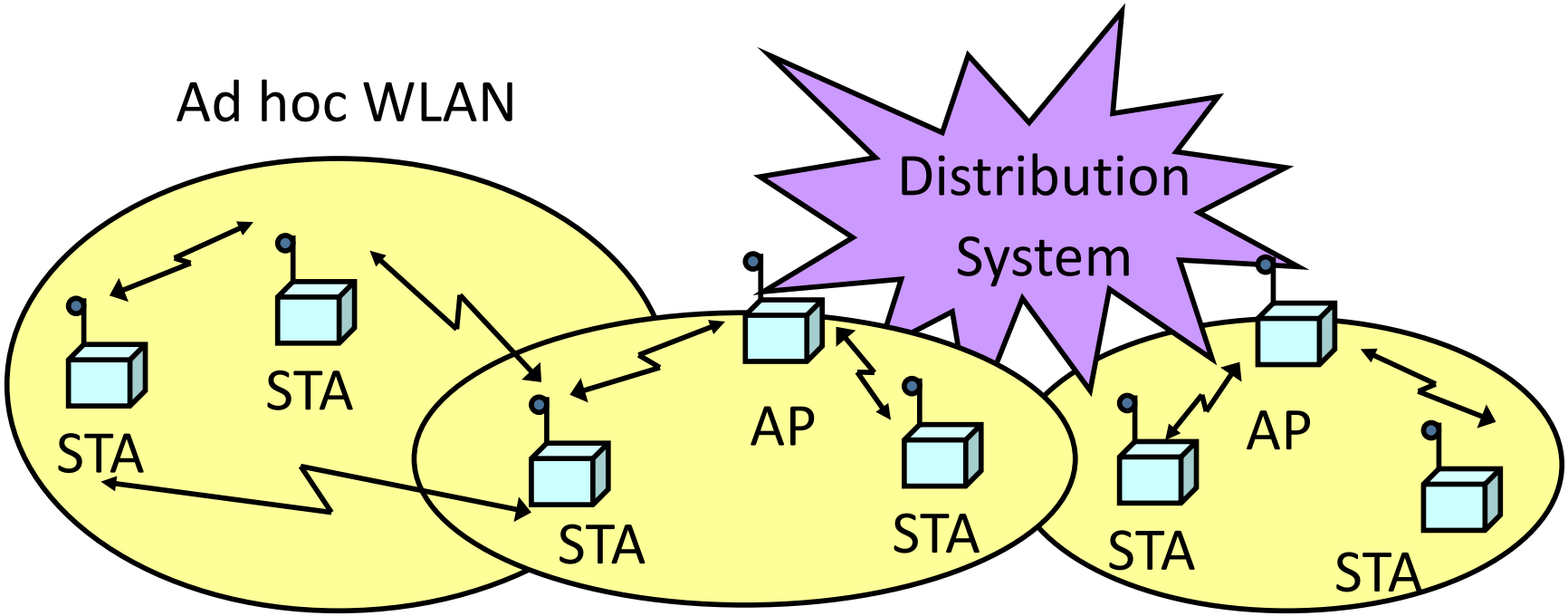
Ad hoc networking
Independent BSS (IBSS)



Network with infrastructure



Possible Scenarios (2)



WLANs with infrastructure

- Between the PHY/MAC and the 802.2 LLC (or IP) there are additional functions for registering one interface to the others
  - With infrastructured systems we say to “join a BSS/AP”
- Without proper association a network is not formed and STA do not communicate
  - Exception: 802.11p → Vehicular Networks

- BSS with AP: Both authentication and association are necessary for joining a BSS
- Independent BSS: Neither authentication neither association procedures are mandatory or specified in the standard an IBSS → ad-hoc, proprietary, none

A station willing to join a BSS must get in contact with the AP. This can happen through:

1. Passive scanning
   - The station scans the channels for a Beacon frame that is periodically (100ms) sent by every AP
2. Active scanning (the station tries to find an AP)
   - The station sends a ProbeRequest frame on a given channel
   - All AP's within reach reply with a ProbeResponse frame

- Active Scanning may be more performing but waste resources

- Beacons are broadcast frames transmitted periodically (default 100ms). They contain:
  - Timestamp
  - TBTT (Target Beacon Transmission Time) – also called Beacon Interval
  - Capabilities
  - SSID (BSSID is AP MAC address + 26 optional octets)
  - PHY layer information
  - System information (Network, Organization, …)
  - Information on traffic management if present
  - …
- STA answer to beacons with a ProbeResponse containing the SSID

- **Directed probe**: The client sends a probe request with a specific destination SSID; only APs with a matching SSID will reply with a probe response
  - It is often considered “secure” if APs do not broadcast SSIDs and only respond to Directed Probes …
- **Broadcast probe**: The client sends a null SSID in the probe request; all APs receiving the probe-request will respond with a probe-response for each SSID they support
  - Useful for service discovery systems

UNIVERSITY OF TRENTO
Department of Information Engineering and Computer Science

Once an AP is found/selected, a station goes through authentication

- Open system authentication
  - Station sends authentication frame with its identity
  - AP sends frame as an ack / nack
- Shared key authentication (WEP)
  - Stations receive shared secret key through secure channel independent of 802.11
  - Stations authenticate because they use the secret key (weak)
- Per Session Authentication (WPA2)
  - Encryption is AES
  - The key can be shared (home networks) or user-based (enterprise)
  - Encryption is always per-station plus one for broadcast

Association

Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming

- STA → AP: AssociateRequest frame
- AP → STA: AssociationResponse frame
- In case of Roaming: New AP informs old AP via DS

- Only after the association is completed, a station can transmit and receive data frames