UNIVERSITA' DEGLI STUDI DI PARMA
Dipartimento di Ingegneria dell'Informazione

Protocolli: strato PH e DL nelle Wireless LAN

Luca Veltri

(mail.to: luca.veltri@unipr.it)
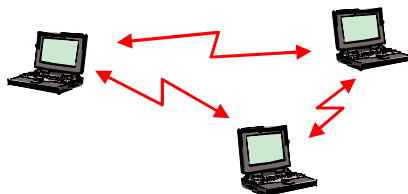
Corso di Reti di Telecomunicazioni A, a.a. 2008/2009

http://www.tlc.unipr.it/veltri

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
WLAN

Wireless LAN Standards

- 802.11 (July 1997)
  - **IEEE specification for 1, 2 Mb/s running in 2.4GHz ISM band (Industrial Scientific and Medical)**
  - **common MAC layer (CSMA/CA)**
  - **different PH layers (FHSS, DSSS)**
- 802.11b (Sept. 1999)
  - **IEEE specification for 11 Mbit/s running at 2.4 GHz (CCK 2.4GHz)**
  - **actually you only get 5.5-8 Mb/s**
  - **Widely adopted**
- 802.11a
  - **IEEE specification for 54 Mbit/s running at 5 GHz (OFDM)**
  - **Not (yet) widely adopted**
- 802.11g
  - **IEEE specification for up to 54 Mbit/s running in 2.4 GHz**

2

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
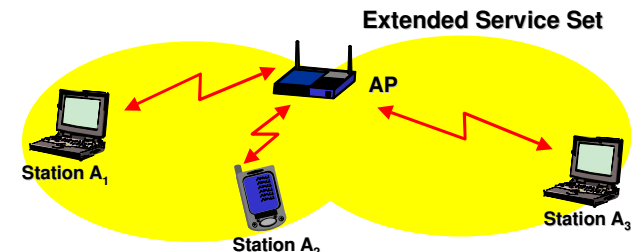WLAN

Had-hoc mode

- Basic Service Set (BSS)
  - **group of stations that are all under the same covered area (i.e. a cell) and that communicate under the same control function (CDF or PCF, see below)**
  - **conceptually all stations in a BSS can communicate directly with each other**
- Ad-hoc network
  - **stations within an Independent Basic Service Set (IBSS)**
  - **only the stations within a common coverage area can communicate with other stations**
  - **If a client in an ad-hoc network wishes to communicate outside of the cell, a member of the cell MUST operate as a gateway and perform routing**
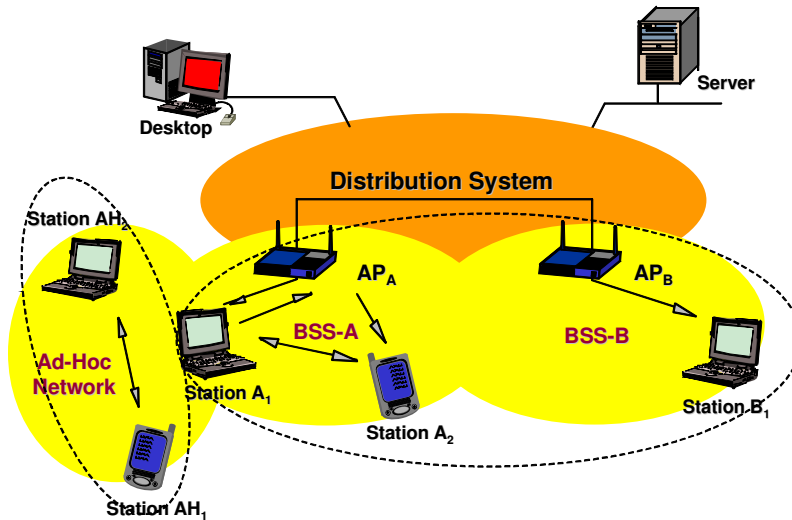
3

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
WLAN

Infrastructure mode

- Infrastructure mode
  - **each client sends all of it's communications to a central station AP (Access Point)**
  - **the access point acts as an Ethernet bridge**
    - forwards the communications (the layer-2 PDU) onto the appropriate network, either wired or wireless

Extended Service Set

AP

Station A$_1$

Station A$_2$

Station A$_3$

4

Ad-hoc and Infrastructure modes

802.11 MAC Layer

- Medium Access Control (MAC) sublayer is responsible for
  - **channel allocation procedures,**
  - **MAC-PDU addressing,**
  - **frame formatting,**
  - **error checking,**
  - **fragmentation and reassembly**
- The medium can operate in
  - **contention mode, know as Contention Period (CP) mode**
  - **contention-free period (CFP) mode**
- During CFP the medium access is controlled by the AP
- The 802.11 MAC is based upon CSMA/CA (Carrier Sense Medium Access with Collision Avoidance)
- Three types of frames
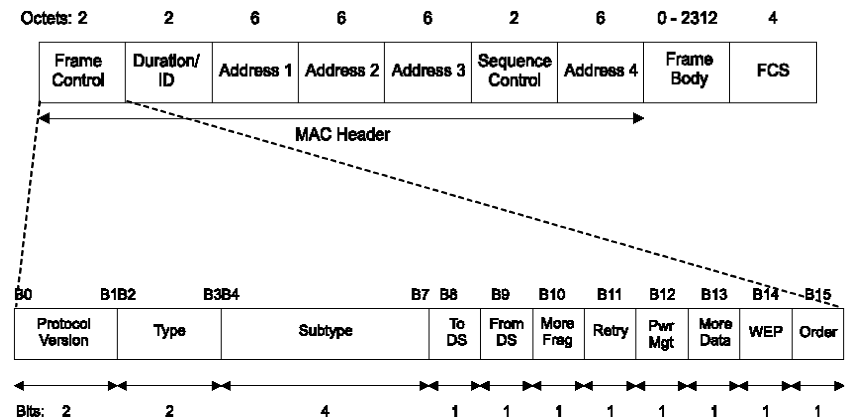 - **management, control, data**

802.11 MAC Layer

- Management frames are used for
  - **association/disassociation with a AP**
  - **timing and synchronization**
  - **authentication**
- Control frames are used for
  - **handshaking during CP**
  - **positive acknowledgment during CP**
  - **to end CFP**
- Data frames are used for
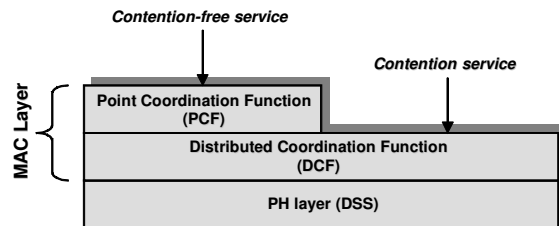 - **transmission of data during CP and CFP, and can be combined with polling and acknowledgment during CFP**

MAC-PDU format

802.11 MAC Layer

- The are two different methods for medium access control
  - **Distributed Coordination Function (DCF)**
  - **Point Coordination Function (PCF)**
- The first method (DCF) is applied only with AP, i.e. in ESS
  - **the medium can work both in CP and CFP**
- The latter is used in ad-hoc network (IBSS)
  - **the medium works only in CP**

Contention-free service

Contention service

MAC Layer

| Point Coordination Function (PCF) |
| Distributed Coordination Function (DCF) |
| PH layer (DSS) |

Distributed Coordination Function (DCF)

- Fundamental access method used to support asynchronous data transfer (must be always supported)
- Is the only access method for Ad-hoc mode
- DCF is a contention access method based on Carrier Sense Multiple Access with collision Avoidance (CSMA/CA)
  - **collision detection (CSMA/CD) is not used due to the inability for a station to listen to the channel while transmitting**
  - **carrier sense is performed both at PH layer (*PH carrier sensing*) and at MAC layer (*virtual carrier sensing*)**
- Virtual carrier sensing is performed by sending MAC-PDU duration information in the header of request to send (RTS), clear to send (CTS), and data frames (see later)

Distributed Coordination Function (DCF)

- The MAC-PDU *duration* field indicates the amount of time (µs) that the channel will be utilized after the transmission of the current frame
- Stations in BSS use the information read in the *duration* field to adjust their "network allocation vector" (NAV) which indicates the amount of time that the channel must considered busy
  - **i.e. the time that must elapse before sampling again the medium for idle status**
- Priority access to the medium is controlled through the use of interframe space (IFS), i.e. the time interval between transmitted frames
- Three IFS are specified in growing order:
  - **short IDS (SIFS)**
  - **point coordination function IFS (PIFS)**
  - **distributed coordination function IFS (DIFS)**

Distributed Coordination Function (DCF)

- Stations only required to wait a SIFS have priority access over those stations required to wait PIFS or DIFS
- For the basic access method, when a station sense (virtually and/or physically) the channel is idle, waits for a DIFS period before sampling the medium again
- if the channel is still idle the station can transmits a MAC-PDU
- The receiver station calculates the checksum and, if correct, waits a SIFS interval and transmit an ACK frame to the originator
- Each station calculate its NAV by reading the *duration* field in the MAC frames
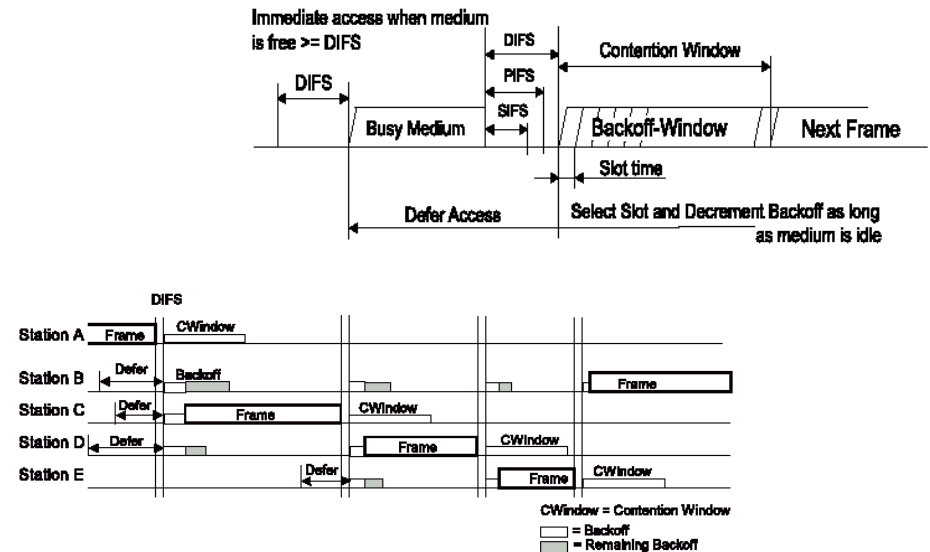 - **the *duration* field in Data frames includes the SIFS and the ACK duration**

Distributed Coordination Function (DCF)

- Since collisions can still occur, before sending a Data frame a station sends a Request To Send (RTS) control frame that should be confirmed by the receiver by a Clear To Send (CTS) control frame

- RTS and CTS are very short frames (20 and 14 respectively)

- If a collision occur (when sending a RTS) no CTS can be sent, and the originator station "detect" the collision and start the backoff

- Collisions can occur only on RTS frames
  - **each station receiving a RTS read the _duration_ field, set its NAV, avoiding any successive collision (the medium becomes reserved)**

- Retransmission attempts use an exponential-backoff time

- The MAC algorithm is fair, however no bound exist for the maximum transmission delay

13

Distributed Coordination Function (DCF)

14

Point Coordination Function (PCF)

- PCF is an optional capability providing contention-free frame transfer (currently, rarely implemented)

- PCF relies on the point coordinator (the AP in each BSS), that polls the stations for enabling them to transmit (without contending for medium access)

- PCF must coexist with the DCF

- A station is not required to support PCF

- The time axes is slotted in contention-free intervals (CFPs) alternate with contention-based intervals (CPs)

- During a contention-free period, no RTS/CTS frames are used; it is the AP that polls the station for possible transmission
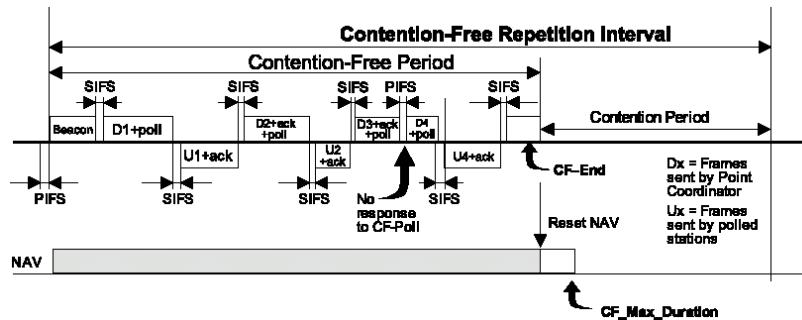
15

Point Coordination Function (PCF)

- At the nominal start of CFP the AP sense the medium and, if idle, wait a PIFS and then initiates the CFP with a "beacon" frame

- Successively, the following frames can be used:
  - **CF-Poll (no data): used by the AP to poll a station**
  - **Data: used to transmit a data frame**
  - **Data+CF-Poll: used by the AP to transmit a frame and poll a station**
  - **CF-ACK: used by a station to confirm to the AP the reception of a data frame (after a SIFS)**
  - **Data+CF-ACK: used by a station to send data after a CF-Poll**
  - **Data+CF-ACK+CF-Pool: used by the AP to confirm a received data (CF-ACK), plus a Data+CF-Poll**
  - **Null (no data): used by station as response to CF-Poll when no data has to be transmitted**
  - **CF-End: used by the AP to end the CFP**

16

Point Coordination Function (PCF)

Client-AP association

● Prior to communicating data, wireless clients and access points must establish a relationship, or an association

● In infrastructure mode, the clients associate with an AP

● How clients find and associate with APs:
  ➢ **All access points transmit a beacon management frame at fixed interval**
  ➢ **To associate with an AP and join a BSS, a client listens for beacon messages to identify the access points within range**
  ➢ **The client then selects the BSS to join in a vendor dependent manner (based on the network names (or service set identifiers (SSID)) which are usually contained in the beacon frame)**
  ➢ **A client may also send a probe request management frame to find an access point affiliated with a desired SSID**
  ➢ **After identifying an access point, the client and the access point perform a mutual authentication by exchanging several management frames as part of the process**

IEEE 802.11 (in)security

● There are currently three basic methods to secure access to an AP that are built into 802.11 networks:
  ➢ **Service set identifier (SSID)**
  ➢ **Media Access Control (MAC) address filtering**
  ➢ **Wired Equivalent Privacy (WEP)**

● One or all of these methods may be implemented (but all three together provide a more robust solution)

SSID

● Service Set ID (SSID)

● Like a network name, usually a human readable string

● A SSID can be associated with an AP or group of APs

● The SSID provides a mechanism to "segment" a wireless network into multiple networks serviced by one or more APs
  ➢ **Each AP is programmed with an SSID corresponding to a specific wireless network**
  ➢ **A building might be segmented into multiple net-works by floor or department**

● To access a network, clients must be configured with the correct SSID
  ➢ **client can be configured with multiple SSIDs**

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
WLAN

SSID

- Effectively a shared secret (password)
  - **originally designed to allow different groups to use different APs**
  - **can be used to restrict the access only to users that provide a correct SSID**
    - a form of network access control
    - the SSID acts as a simple password

- Problems
  - **A widely shared secret**
    - everyone using the network needs to now it
    - SSIDs are widely known and easily shared
  - **Plaintext secret**
  - **The secret is compromised if the AP is configured to "broadcast" its SSID**
    - Broadcast periodically from the AP

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
WLAN

MAC address filtering

- If we know which clients are authorized to use the AP, let's just list their MAC addresses in an ACL

- Problems
  - **Scalability**
  - **MAC addresses can be spoofed**
  - **Physical security**
    - Someone steals your NIC, they are authorized

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
WLAN

MAC Address Filtering

- A client computer can be identified by the unique MAC address

- To increase the security of an 802.11 network, each AP can be pro-grammed with a list of MAC addresses associated with the clients allowed to access the AP

- MAC address filtering (along with SSIDs) provides improved security, but is best suited to small networks where the MAC address list can be efficiently managed
  - **Each AP must be manually programmed with a list of MAC addresses, and the list must be kept up-to-date**
  - **This administrative overhead limits the scalability of this approach**

Università degli Studi di Parma
Dipartimento di Ingegneria dell'Informazione
WLAN

Wired Equivalency Protocol

- WEP is the standard mechanism for ensuring data confidentiality over wireless networks

- According to the name, it is supposed to provide security equivalent to that of a wired network
  - **Unfortunately it is badly broken**
  - **Wired networks aren't that secure anyways**