Lecture 13

IEEE 802.11 Architecture

The standard is similar in most respects to the IEEE 802.3 Ethernet standard. Specifically, the 802.11 standard addresses:

- Functions required for an 802.11 compliant device to operate either in a peer-to-peer fashion or integrated with an existing wired LAN
- Operation of the 802.11 device within possibly overlapping 802.11 wireless LANs and the mobility of this device between multiple wireless LANs
- MAC level access control and data delivery services to allow upper layers of the 802.11 network
- Several physical layer signaling techniques and interfaces
- Privacy and security of user data being transferred over the wireless media

In 1997 the IEEE adopted IEEE Std. 802.11-1997, the first wireless LAN (WLAN) standard. This standard defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless connectivity. It addresses local area networking where the connected devices communicate over the air to other devices that are within close proximity to each other.

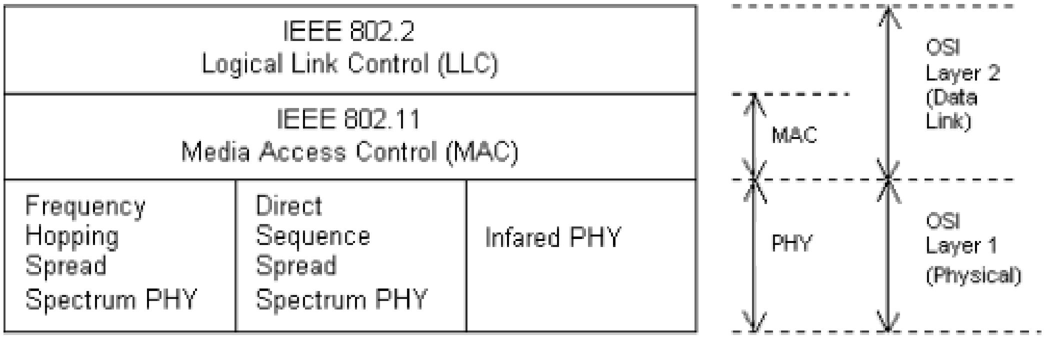

IEEE 802.2
Logical Link Control (LLC)
IEEE 802.11
Media Access Control (MAC)
Frequency Hopping Spread Spectrum PHY
Direct Sequence Spread Spectrum PHY
Infared PHY
MAC
PHY
OSI Layer 2 (Data Link)
OSI Layer 1 (Physical)

Figure 1 - IEEE 802.11 standards mapped to the OSI reference model.

The 802.11 architecture is comprised of several components and services that interact to provide station mobility transparent to the higher layers of the network stack.

Wireless LAN Station

The *station* (STA) is the most basic component of the wireless network. A station is any device that contains the functionality of the 802.11 protocol, that being MAC, PHY, and a connection to the wireless media. Typically the 802.11 functions are implemented in the hardware and software of a network interface card (NIC).

A station could be a laptop PC, handheld device, or an Access Point. Stations may be mobile, portable, or stationary and all stations support the 802.11 station services of authentication, de-authentication, privacy, and data delivery.

Basic Service Set (BSS)

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells. Each cell (called **Basic Service Set,** or **BSS**, in the 802.11 nomenclature) is controlled by a Base Station
(Called **Access Point** or, in short, **AP**), which is also a part of BSS. It is also known as Infrastructural Basic Service Set.

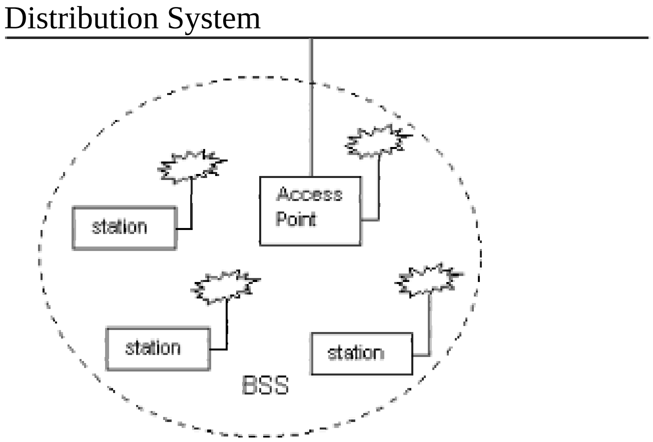


Figure 3 - Infrastructure Basic Service Set

Independent Basic Service Set (IBSS)

The most basic wireless LAN topology is a set of stations, which have recognized each other and are connected via the wireless media in a peer-to-peer fashion. This form of network topology is referred to as an *Independent Basic Service Set* (IBSS) or an *Ad-hoc* network.

In an IBSS, the mobile stations communicate directly with each other. Every mobile station may not be able to communicate with every other station due to the range limitations. There are no relay functions in an IBSS therefore all stations need to be within range of each other and communicate directly.

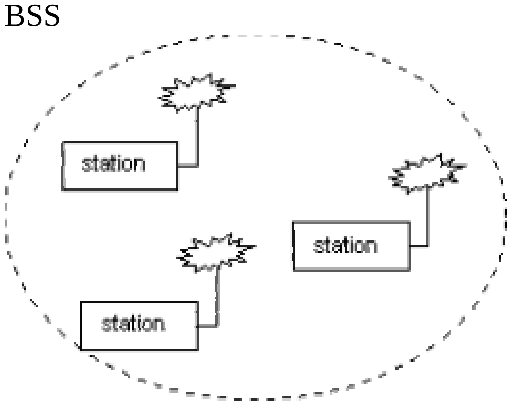


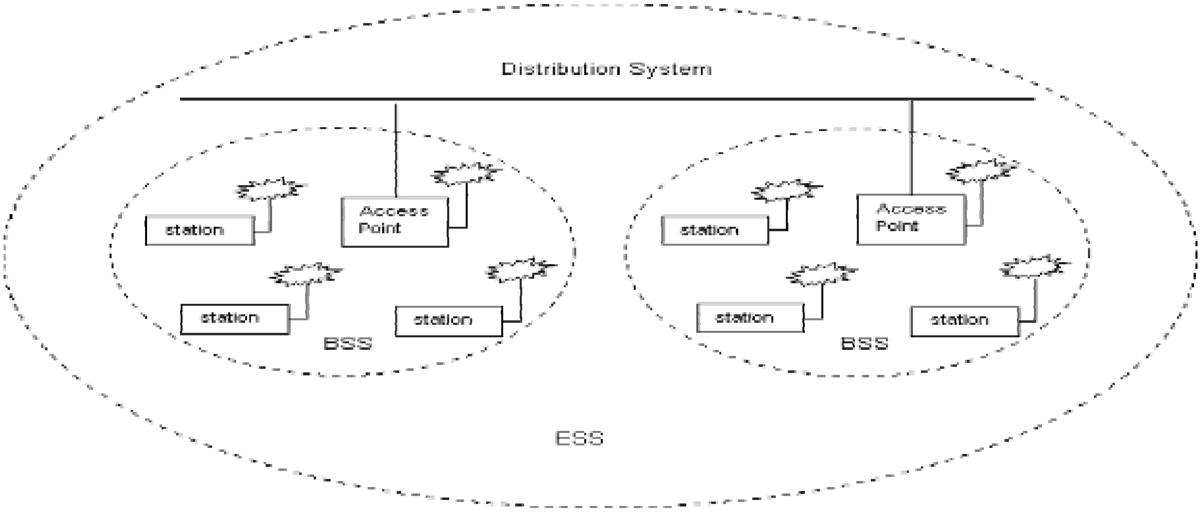
Figure 2 - Independent Basic Service Set (IBSS)

***Distribution System** (DS)* The *distribution system* (DS) is the means by which an access point communicates with another access point to exchange frames for stations in their respective BSSs, forward frames to follow mobile stations as they move from one BSS to another, and exchange frames with a wired network

As IEEE 802.11 describes it, the distribution system is not necessarily a network nor does the standard place any restrictions on how the distribution system is implemented, only on the services it must provide. Thus the distribution system may be a wired network like 802.3 or a special purpose box that interconnects the access points and provides the required distribution services.

Extended Service Set (ESS) 802.11 extends the range of mobility to an arbitrary range through the *Extended Service Set* (ESS). An extended service set is a set of infrastructure BSS's, where the access points communicate amongst themselves to forward traffic from one BSS to another to facilitate movement of stations between BSS's..

The access point performs this communication through the distribution system. The distribution system is the backbone of the wireless LAN and may be constructed of either a wired LAN or wireless network.



The standard also defines a concept of **Portal**. A portal is a device that interconnects between an 802.11 and another 802 LAN. This concept is an abstract description of part of the functionality of a "translation bridge".

802.11 Media Access Control

The 802.11 MAC provides a controlled access method to the shared wireless media called *Carrier-Sense Multiple Access with Collision Avoidance* (CSMA/CA). CSMA/CA is similar to the collision detection access method deployed by 802.3 Ethernet LANs.

The second function of the 802.11 MAC is to protect the data being delivered by providing security and privacy services. Security is provided by the authentication services and by *Wireless Equivalent Privacy* (WEP), which is an encryption service for data delivered on the WLAN

The MAC Layer defines two different access methods,

- Distributed Coordination Function
- Point Coordination Function

Distribution Coordination Function

The basic access mechanism, called the **Distributed Coordination Function**, is basically a Carrier Sense Multiple Access with Collision Avoidance mechanism (usually known as **CSMA/CA**).

A CSMA protocol works as follows: A station desiring to transmit senses the medium. If the medium is busy (i.e. some other station is transmitting) then the station defers its transmission to a later time. If the medium is sensed free then the station is allowed to transmit. These kinds of protocols are very effective when the medium is not heavily loaded since it allows stations to transmit with minimum delay. But there is always a chance of stations simultaneously sensing the medium as being free and transmitting at the same time, causing a collision.

These collision situations must be identified so the MAC layer can retransmit the packet by itself and not by upper layers, which would cause significant delay. In the Ethernet case this collision is recognized by the transmitting stations which go into a retransmission phase based on an **exponential random back-off** algorithm.

<u>While these Collision Detection mechanisms are a good idea on a wired LAN, they cannot be used on a Wireless LAN environment for two main reasons</u>:
1. Implementing a Collision Detection Mechanism would require the implementation of a **Full Duplex radio capable of transmitting and receiving at once**, an approach that would increase the price significantly.
2. In a Wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the Collision Detection scheme), and the fact that a station wants to transmit and senses the medium as free doesn't necessarily mean that **the medium is free around the receiver area**.

In order to overcome these problems, the 802.11 uses a **Collision Avoidance (CA)** mechanism together with a Positive Acknowledge scheme, as follows:
1. A station wanting to transmit senses the medium. If the medium is busy then it defers. If the medium is free for a specified time (called Distributed Inter Frame Space (DIFS) in the standard), then the station is allowed to transmit.

2. The receiving station checks the CRC of the received packet and sends an acknowledgment packet (ACK). Receipt of the acknowledgment indicates to the transmitter that no collision occurred. If the sender does not receive the acknowledgment then it retransmits the fragment until it receives acknowledgment or is thrown away after a given number of retransmissions.

In order to reduce the probability of two stations colliding because they cannot hear each other, the standard defines a Virtual Carrier Sense mechanism:

1. A station wanting to transmit a packet first transmits a short control packet called **RTS** (Request to Send), which includes the source, destination, and the duration of the following transaction (i.e. the packet and the respective **ACK**), the destination station responds (if the medium is free) with a response control Packet called **CTS** (Clear to Send), which includes the same duration information.

2. All stations receiving either the RTS and/or the CTS, set their **Virtual Carrier Sense** indicator (called **NAV**, for **Network Allocation Vector**), for the given duration, and use this information together with the Physical Carrier Sense when sensing the medium.

This mechanism reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter to the short duration of the RTS transmission because the station hears the CTS and “reserves” the medium as busy until the end of the transaction. The duration information on the RTS also protects the transmitter area from collisions during the ACK (from stations that are out of range of the acknowledging station).

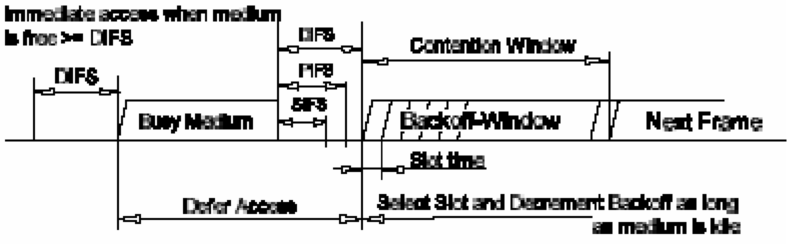

Immediate access when medium is free >= DIFS
DIFS
DIFS
PIFS
SIFS
Contention Window
Busy Medium
Backoff-Window
Next Frame
Slot time
Defer Access
Select Slot and Decrement Backoff as long as medium is idle

Figure 4: Access Mechanism

Exponential Back-off Algorithm

Back-off is a well known method used to resolve contention between different stations wanting to access the medium. The method requires each station to choose a Random Number (n) between 0 and a given number, and wait for this number of Slots before accessing the medium, always checking if a different station has accessed the medium before.

The **Slot Time** is defined in such a way that a station will always be capable of determining if another station has accessed the medium at the beginning of the previous slot. This reduces collision probability by half.

Exponential Back-off means that each time the station chooses a slot and happens to collide, it will increase the maximum number for the random selection exponentially.

The 802.11 standard defines an **Exponential Back-off Algorithm** that must be executed in the following cases:

- When the station senses the medium before the first transmission of a packet, and the medium is busy.
- After each retransmission, and
- After a successful transmission

The only case when this mechanism is not used is when the station decides to transmit a new packet and the medium has been free for more than DIFS.

The above figure shows a schematic of the access mechanism:

Point Coordination Function

Beyond the basic Distributed Coordination Function, there is an optional Point Coordination Function, which may be used to implement time-bounded services, like voice or video transmission.

This Point Coordination Function makes use of the higher priority that the Access Point may gain by the use of a smaller Inter Frame Space (PIFS).

By using this higher priority access, the Access Point issues polling requests to the stations for data transmission, hence controlling medium access. In order to still enable regular stations to access the medium, there is a provision that the Access Point must leave enough time for Distributed Access in between the PCF.