



UNIVERSITA' DEGLI STUDI DI BERGAMO
Facoltà di Ingegneria

Informatica Industriale

Prof. Davide Brugali

3.4 – Wireless LAN

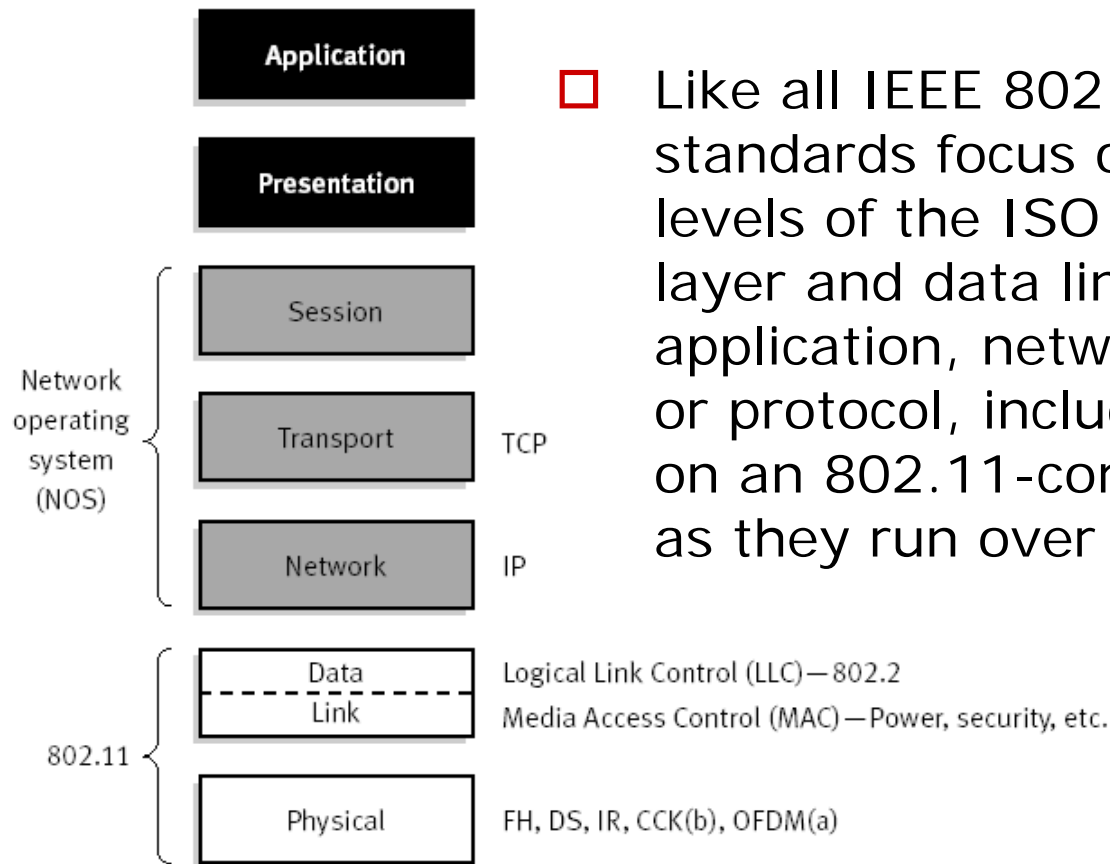
Definition

- ❑ A wireless LAN (WLAN) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure.
- ❑ In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network across a building or campus setting.

Standard

- ❑ The Institute of Electrical and Electronics Engineers (IEEE) ratified the original 802.11 specification in 1997 as the standard for wireless LANs.
- ❑ That version of 802.11 provides for 1 Mbps and 2 Mbps data rates and a set of fundamental signaling methods and other services.
- ❑ IEEE recently ratified the 802.11b standard (also known as 802.11 High Rate) for transmissions of up to 11 Mbps.

ISO – OSI Model

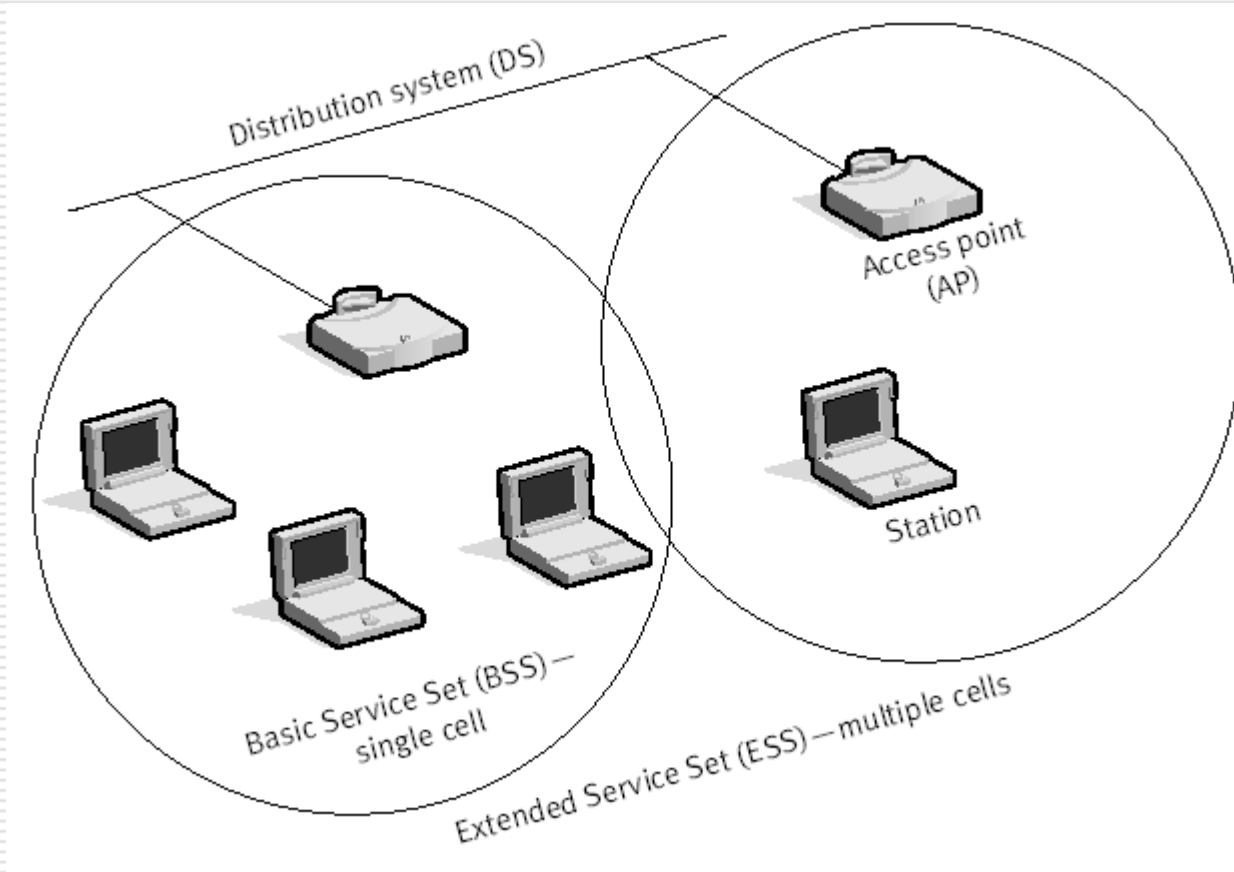


- Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels of the ISO model, the physical layer and data link layer. Any LAN application, network operating system, or protocol, including TCP/IP, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

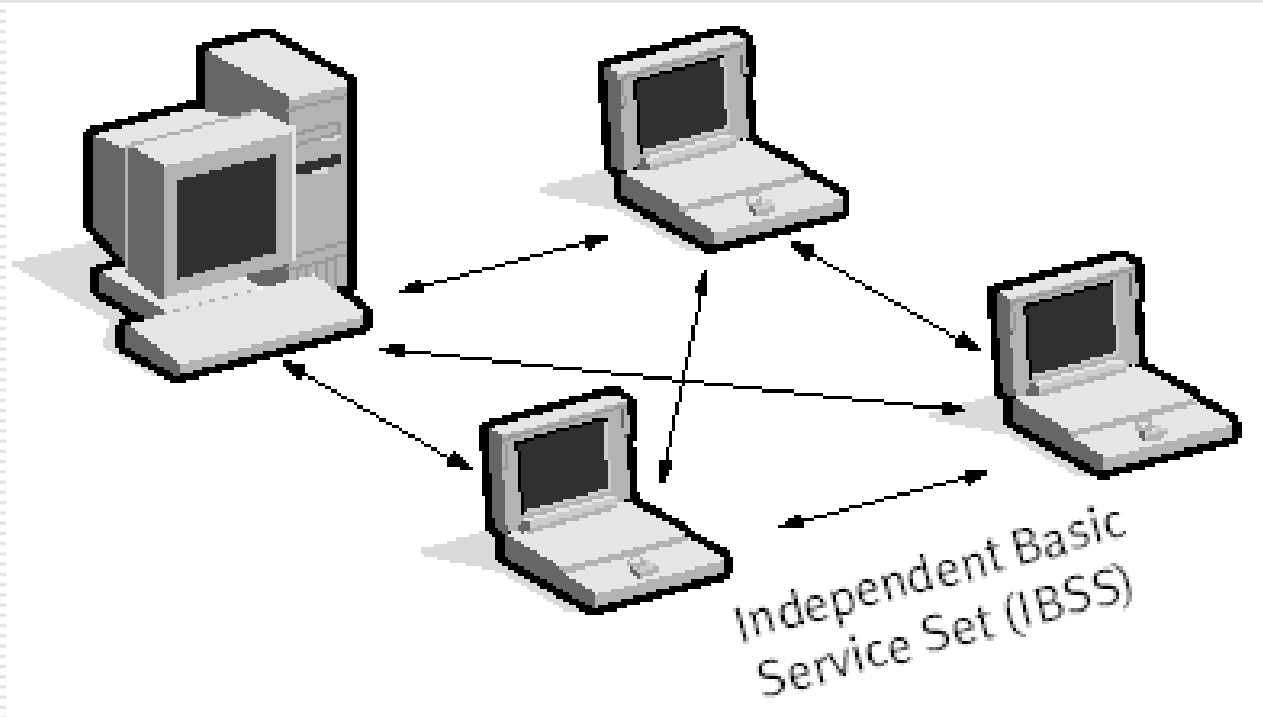
802.11 Operating Modes

- 802.11 defines two pieces of equipment
 - a **wireless station**, which is usually a PC equipped with a wireless network interface card (NIC)
 - and an **access point (AP)**, which acts as a bridge between the wireless and wired networks.
- An access point usually consists of a radio, a wired network interface (e.g., 802.3), and bridging software conforming to the 802.1d bridging standard.
- The access point acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network.

Infrastructure Mode



Ad hoc Mode



Layer 1 : Physical Layer

- The three physical layers originally defined in 802.11 included
 - Infrared
 - Radio Frequency
 - Microwave

- In 1985 the United States released the industrial, scientific, and medical (ISM) frequency bands.
 - 902 - 928MHz
 - 2.4 - 2.4853 GHz
 - 5.725 - 5.85 GHz

- The radio-based standards operate within the 2.4 GHz ISM band.
- These frequency bands are recognized by international regulatory agencies, such as the FCC (USA), ETSI (Europe), and the MKK (Japan) for unlicensed radio operations

Infrared

- ❑ Simple in design and therefore inexpensive.
- ❑ Use the same signal frequencies used on fiber optic links. IR systems detect only the amplitude of the signal and so interference is greatly reduced.
- ❑ Not bandwidth limited and thus can achieve transmission speeds greater than the other systems.
- ❑ Aimed : range of a couple of kilometer
- ❑ Omnidirectional : 10- 30 meters
- ❑ Drawbacks to IR systems:
 - the transmission spectrum is shared with the sun
 - require an unobstructed line of sight (LOS).

Microwave

- ❑ Microwave (MW) systems operate at **less than 500 milliwatts** of power in compliance with FCC regulations.
- ❑ MW systems are by far the fewest on the market. They use narrow-band transmission with single frequency modulation and are set up mostly in the **5.8GHz band**.
- ❑ The big advantage to MW systems is **higher throughput** achieved because they do not have the overhead involved with spread spectrum systems.
- ❑ RadioLAN is an example of systems with microwave technology.

RADIO - Signaling mechanisms

- ❑ The original 802.11 wireless standard defines data rates of 1 Mbps and 2 Mbps via radio waves using
 - frequency hopping spread spectrum (FHSS) or
 - direct sequence spread spectrum (DSSS).

- ❑ It is important to note that FHSS and DSSS are fundamentally different signaling mechanisms and will not interoperate with one another.

Frequency hopping

- ❑ The 2.4 - 2.4853 GHz band is divided into 75 1-MHz subchannels.
- ❑ The sender and receiver agree on a hopping pattern, and data is sent over a sequence of the subchannels.
- ❑ Each conversation within the 802.11 network occurs over a different hopping pattern, and the patterns are designed to minimize the chance of two senders using the same subchannel simultaneously.

Frequency Hopping

- ❑ FHSS techniques allow for a relatively simple radio design, but are limited to speeds of no higher than 2 Mbps.
- ❑ This limitation is driven primarily by FCC regulations that restrict subchannel bandwidth to 1 MHz.
- ❑ These regulations force FHSS systems to spread their usage across the entire 2.4 GHz band, meaning they must hop often, which leads to a high amount of hopping overhead.

Direct Sequence Signaling

- ❑ In contrast, the direct sequence signaling technique divides the 2.4 GHz band into 14 22-MHz channels.
- ❑ Adjacent channels overlap one another partially, with 3 of the 14 being completely non-overlapping.
- ❑ Data is sent across one of these 22 MHz channels without hopping to other channels. To compensate for noise on a given channel, a technique called “chipping” is used.
- ❑ Each bit of user data is converted into a series (called a Barker sequence) of 11-20 redundant bit patterns called “chips.”
- ❑ The inherent redundancy of each chip combined with spreading the signal across the 22 MHz channel provides for a form of error checking and correction; even if part of the signal is damaged, it can still be recovered in many cases, minimizing the need for retransmissions.

802.11b

Enhancements to the PHY Layer

- ❑ Two new speeds, 5.5 Mbps and 11 Mbps with DSSS only.

- ❑ These symbols are transmitted at a 1 MSps (1 million symbols per second) symbol rate using a technique called Binary Phase Shift Keying (BPSK).

- ❑ In the case of 2 Mbps, a more sophisticated implementation called Quadrature Phase Shift Keying (QPSK) is used; it doubles the data rate available in BPSK, via improved efficiency in the use of the radio bandwidth.

802.11b

Enhancements to the PHY Layer

- ❑ To increase the data rate, rather than the two 11-bit Barker sequences, 802.11b specifies **Complementary Code Keying (CCK)**, which consists of a set of 64 8-bit code words.
- ❑ As a set, these code words have **unique mathematical properties** that allow them to be correctly distinguished from one another by a receiver even in the presence of substantial noise and multipath interference (e.g., interference caused by receiving multiple radio reflections within a building).
- ❑ The 5.5 Mbps rate uses CCK to encode 4 bits per carrier, while the 11 Mbps rate encodes 8 bits per carrier.
- ❑ Both speeds use QPSK as the modulation technique and signal at 1.375 MSps.

802.11b Data Rate Specifications

Data Rate	Code Length	Modulation	Symbol Rate	Bits/ Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Layer 2 : Data Link Layer

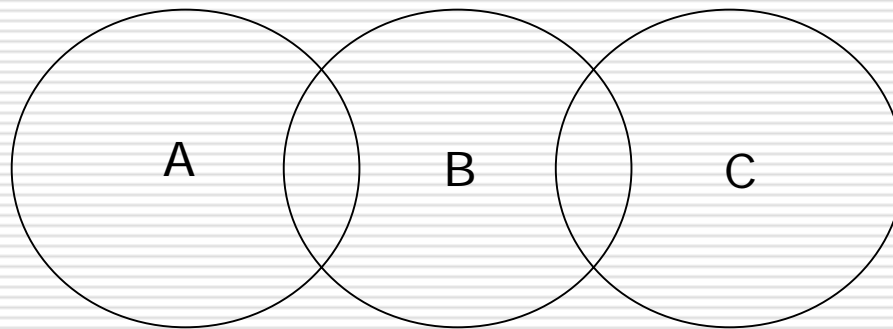
- The data link layer within 802.11 consists of two sublayers:
 - Logical Link Control (LLC) and
 - Media Access Control (MAC).
- 802.11 uses the same 802.2 LLC and 48-bit addressing as other 802 LANs, allowing for very simple bridging from wireless to IEEE wired networks, but the MAC is unique to WLANs.
- The 802.11 MAC is very similar in concept to 802.3, in that it is designed to support multiple users on a shared medium by having the sender sense the medium before accessing it.

Medium Access Control Protocol

- ❑ Most wired LANs products use **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** as the MAC protocol.
- ❑ Carrier Sense means that the station will listen before it transmits. If there is already someone transmitting, then the station waits and tries again later. If no one is transmitting then the station goes ahead and sends what it has.
- ❑ But what if two stations send at the same time? The transmissions will collide and the information will be lost.
- ❑ This is where Collision Detection Comes into play. The station will listen to ensure that its transmission made it to the destination without collisions.
- ❑ If a collision occurred then the stations wait and try again later. The time the station waits is determined by the backoff algorithm.

Medium Access Control Protocol

- The Hidden Node problem: Node C cannot hear node A. So if node A is transmitting, node C will not know and may transmit as well. This will result in collisions.

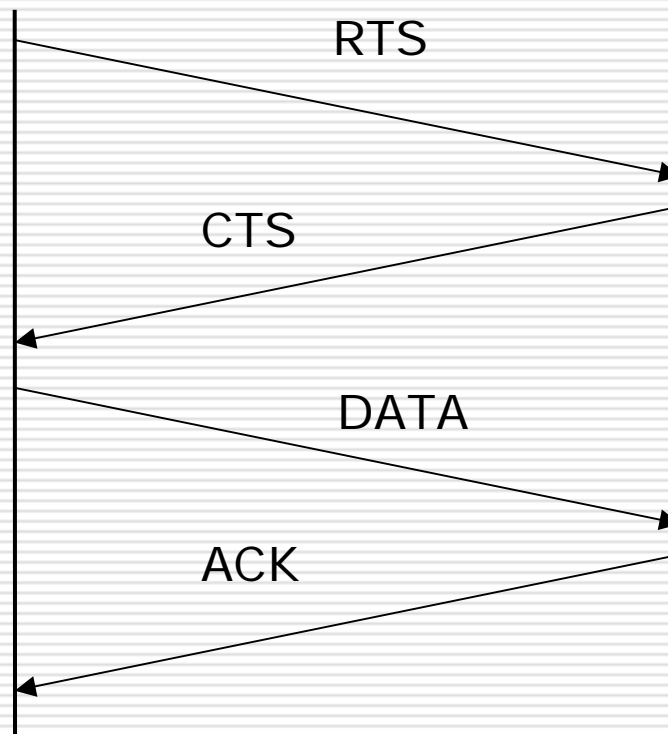


Medium Access Control Protocol

- ❑ **Carrier Sense Multiple Access with Collision Avoidance or CSMA/CA.**
 - the station listens before it sends.
 - If someone is already transmitting, wait for a random period and try again.
 - If no one is transmitting then it sends a short message.
 - This message is called the **Ready To Send message (RTS)**. This message contains the **destination** address and the **duration** of the transmission.
 - Other stations now know that they must wait that long before they can transmit.
 - The destination then sends a short message which is the **Clear To Send message (CTS)**. This message tells the source that it can send without fear of collisions.
 - Each packet is acknowledged. If an acknowledgement is not received, the MAC layer retransmits the data.

Medium Access Control Protocol

□ *The 4-way Handshake*



Medium Access Control Protocol

□ Association

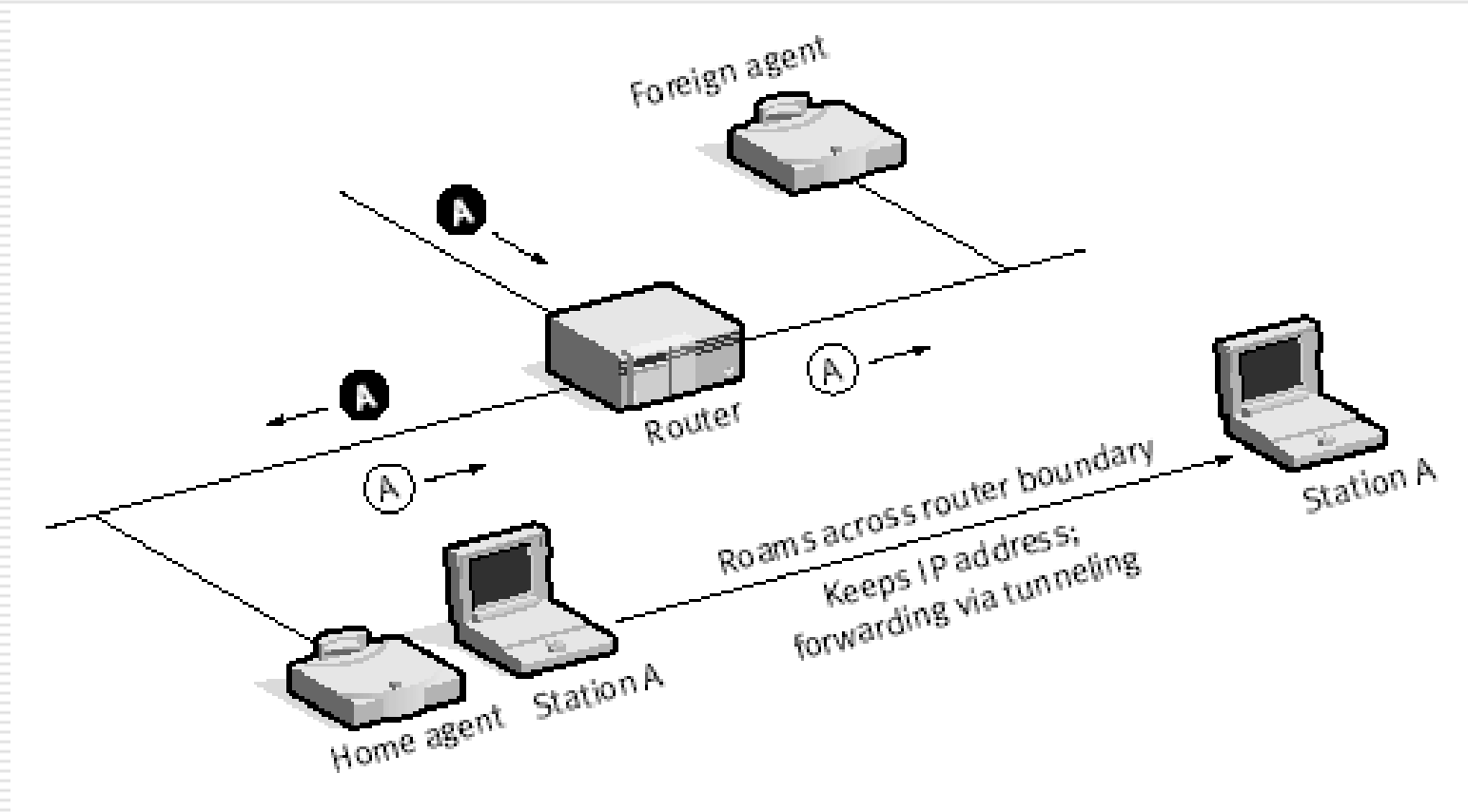
- The 802.11 MAC layer is responsible for how a client associates with an access point. When an 802.11 client enters the range of one or more APs, it chooses an access point to associate with (also called **joining a Basic Service Set**), based on signal strength and observed packet error rates.
- Once accepted by the access point, **the client tunes to the radio channel** to which the access point is set.
- Periodically it surveys all 802.11 channels in order to assess whether a different access point would provide it **with better performance characteristics**. If it determines that this is the case, it reassociates with the new access point, tuning to the radio channel to which that access point is set

Medium Access Control Protocol

□ Roaming

- Reassociation usually occurs because the wireless station has physically **moved away** from the original access point, causing the signal to weaken.
- In other cases, reassociation occurs due to a change in **radio characteristics** in the building
- or due simply to **high network traffic** on the original access point. In this case this function is known as “load balancing,” since its primary function is to distribute the total WLAN load most efficiently across the available wireless infrastructure.

Layer 3 : Mobile IP



Layer 3 : Mobile IP

- ❑ Currently known as RFC 2002 in the Internet Engineering Task Force (IETF).
- ❑ Mobile IP works by having an **access point assigned as the “home agent” for each user.**
- ❑ Once a wireless station leaves the home area and enters a new area, the new access point queries the station for its home agent.
- ❑ Once it has been located, a packet forwarding is established automatically between the two access points to ensure that the user's IP address is preserved and that the user can transparently receive his or her data.
- ❑ As Mobile IP is not finalized, vendors may provide their own protocols using similar techniques to ensure that IP traffic follows a user across networks separated by a router (e.g., across multiple buildings).

Layer 3 : Mobile IP

□ Mobile Node (MN):

A host or router that may change its point of attachment from one network or subnetwork to another through the internet. This entity is pre-assigned a fixed home address on a home network, which other correspondent hosts will use to address their packets to, regardless of its current location.

Layer 3 : Mobile IP

□ Home Agent (HA):

A router that maintains a list of registered mobile nodes in a visitor list. It is used to forward mobile node-addressed packets to the appropriate local network when the mobile nodes are away from home.

□ Foreign Agent (FA):

A router that assists a locally reachable mobile node that is away from its home network. It delivers information between the mobile node and the home agent.

Layer 3 : Mobile IP

□ Home Address:

A permanent IP address that is assigned to a mobile node. It remains unchanged regardless of where the mobile node is attached to the internet.

□ Care-of-address (COA):

An address which identifies the mobile node's current location. It can be either assigned dynamically or associated with its foreign agent.

Layer 3 : Mobile IP

□ **Agent Discovery:**

Home agents and foreign agents broadcast their availability on each link to where they can provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present.

□ **Registration:**

When the mobile node is away from home, it registers its care-of-address with its home agent so that the home agent knows where to forward its packets. Depending on the network configuration, the mobile node could either register directly with its home agent, or indirectly via the help of its foreign agent.

Layer 3 : Mobile IP

□ **In service:**

This is the period after the registration process and before the service time expiration, provided that the mobile node stays in the service area. During service time, the mobile node gets forwarded packets from its foreign agent which were originally sent from the mobile node's home agent.

□ **Deregistration:**

After the mobile node returns home, it deregisters with its home agent to drop its registered care-of-address. In other words, it sets its care-of-address back to its home address.

Layer 3 : Mobile IP

□ Indirect routing:

Consider that if a mobile node happens to move to the same subnetwork as its correspondent node that wants to send it datagrams, this is what will happen in order for the datagram to be received by the mobile node, based on the base Mobile IP protocol:

- the correspondent node will send the datagram all the way to the mobile node's home agent, which may be a half globe away;
- its home agent will then forward the datagram to its care-of-address, which might just take a half second to reach if the datagram is sent directly from the correspondent node.