WiFi modes of operation (802.11 or Wi-Fi)

There are several kinds of hardware that may be used to implement a WiFi wireless network:

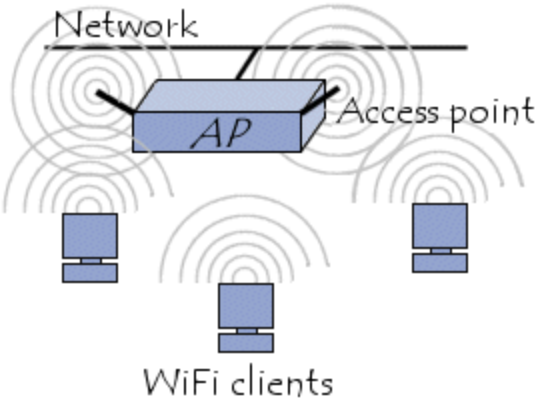
- **Wireless adapters** or **network interface controllers** (NICs for short) are network cards with the 802.11 standard which let a machine connect to a wireless network. WiFi adapters are available in numerous formats, such asPCI cards, PCMCIA cards, USB adapters, and CompactFlash cards. A**station** is any device that has such a card.
- **Access points** (**AP** for short; sometimes called *hotspots*) can let nearby wifi-equipped stations access a wired network to which the access point is directly connected.

The 802.11 standard defines two operating modes:

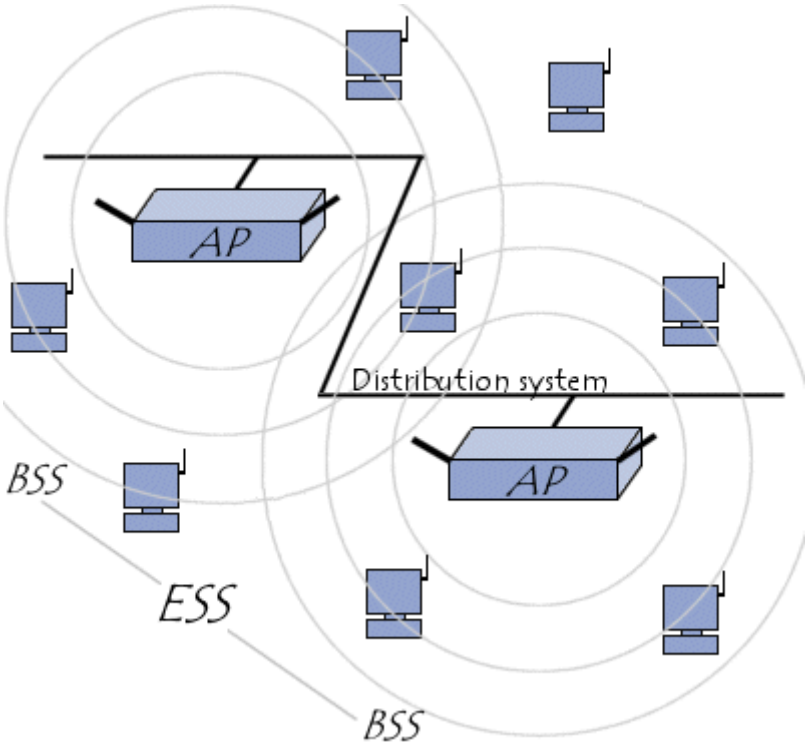
- Infrastructure mode, in which wireless clients are connected to an access point. This is generally the default mode for 802.11b cards.
- Ad hoc mode, in which clients are connected to one another without any access point.

Infrastructure mode

In **mode infrastructure**, each station computer (**STA** for short) connects to an access point via a wireless link. The set-up formed by the access point and the stations located within its coverage area are called the *basic service set*, or **BSS**for short. They form one cell. Each BSS is identified by a BSSID, a 6-byte (48-bite) identifier. In *infrastructure* mode, the BSSID corresponds to the access point's MAC address.



It is possible to link several access points together (or more precisely several BSS's) using a connection called a *distribution system* (**DS** for short) in order to form an *extended service set* or *ESS*. The distribution system can also be a wired network, a cable between two access points or even a wireless network.



An ESS is identified with an **ESSID** (Extended Service Set Identifier), a 32-character identifier (in ASCII format) which acts as its name on the network. The ESSID, often shortened to **SSID**, shows the network's name, and in a way acts a first-level security measure, since it is necessary for a station to know the **SSID**in order to connect to the extended network.

When a roaming user goes from one BSS to another while moving within the ESS, his or her machine's wireless network adapter is able to switch access points depending on the quality of the signal it receives from different access points. Access points communicate with one another using a distribution system in order to trade information about the stations and, if necessary, to transmit data from mobile stations. This feature which lets stations move "transparently" from one access point to another is called **roaming**.

Communicating with the access point

When a station joins a cell, the cell sends a *probe request* on each channel. This request contains the ESSID that the cell is configured to use, as well as the traffic volume that its wireless adapter can support. If no ESSID is set, the station listens to the network for an SSID.

Each access point broadcasts at regular intervals (about ten times a second) a signal called a **beacon**, which gives information on its BSSID, its characteristics, and, if

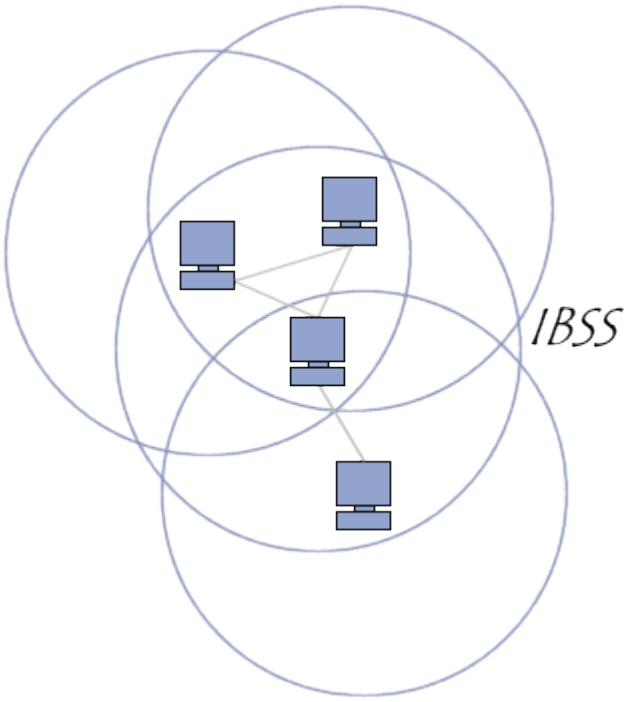
applicable, its ESSID. The ESSID is automatically broadcast by default, but it is possible (and recommended) to disable this option.
Whenever a probe request is received, the access point checks the ESSID and the traffic volume request found in the beacon. If the given ESSID matches that of the access point, the acces point sends a response containing synchronization data and information on its traffic load. This way, the station that receives the response can check the quality of the signal being sent by the access point in order to determine how far away it is. Generally speaking, the closer an access point is, the higher its data transfer capacity is.

So a station within range of multiple access points (which have the same SSID) may **choose** the access point offering the best balance of capacity and current traffic load.

	When a station is within range of several access points, the station chooses which one to connect to.

Ad hoc mode

In **ad hoc mode**, wireless client machines connect to one another in order to form a peer-to-peer network, i.e. a network in which every machine acts as both a client and an access point at the same time.



The set-up formed by the stations is called the **independent basic service set**, or IBSS for short.

An IBSS is a wireless network which has at least two stations and uses no access point. The IBSS therefore forms a temporary network which lets people in the same room exchange data. It is identified by an SSID, just like an ESS in infrastructure mode.

In an ad hoc network, the range of the *independent BSS* is determined by each station's range. That means that if two of the stations on the network are outside each other's range, they will not be able to communicate, even if they can "see" other stations. Unlike infrastructure mode, ad hoc mode has no distribution system that can send data frames from one station to another. An IBSS, then, is by definition a restricted wireless network.

Source: http://en.kioskea.net/contents/804-wifi-modes-of-operation-802-11-or-wi-fi