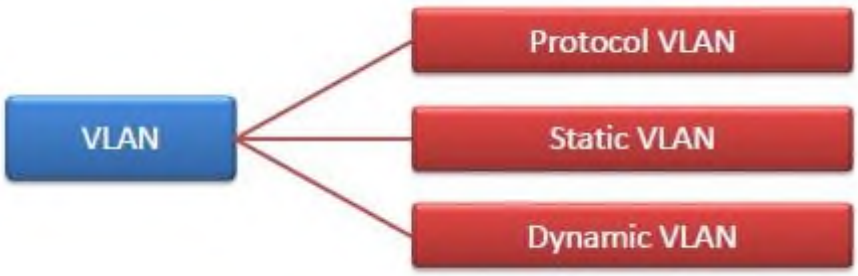
5.11 VLAN

Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network. Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

Features of VLANs

- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.
- VLANs help large organizations to re-partition devices aiming improved traffic management.

Types of VLANs



Protocol VLAN − Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.

Port-based VLAN − This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.

Dynamic VLAN − Here, the network administrator simply defines network membership according to device characteristics.

5.12 WIRELESS LAN (IEEE 802.11)

- Wireless communication is one of the fastest-growing technologies.
- The demand for connecting devices without the use of cables is increasing everywhere.
- Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

ADVANTAGES OF WLAN / 802.11

1. Flexibility: Within radio coverage, nodes can access each other as radio waves can penetrate even partition walls.
2. Planning : No prior planning is required for connectivity as long as devices follow standard convention
3. Design : Allows to design and develop mobile devices.
4. Robustness : Wireless network can survive disaster. If the devices survive, communication can still be established.

TECHNOLOGY USED IN WLAN / 802.11

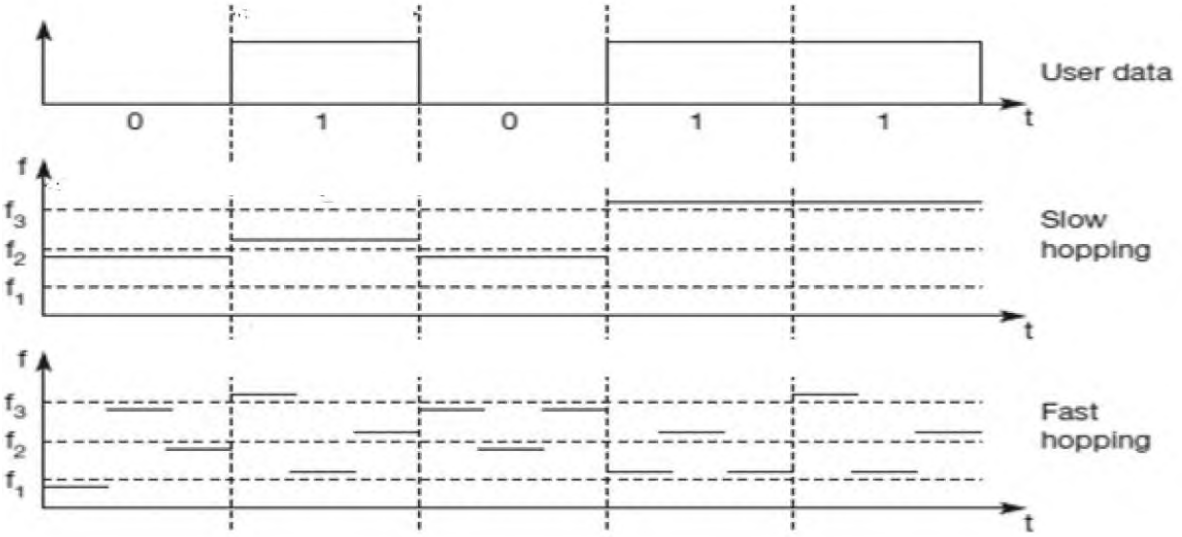
- WLAN's uses Spread Spectrum (SS) technology**.**
- The idea behind Spread spectrum technique is to spread the signal over a wider frequency band than normal, so as to minimize the impact of interference from other devices.
- There are two types of Spread Spectrum:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct **S**equence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

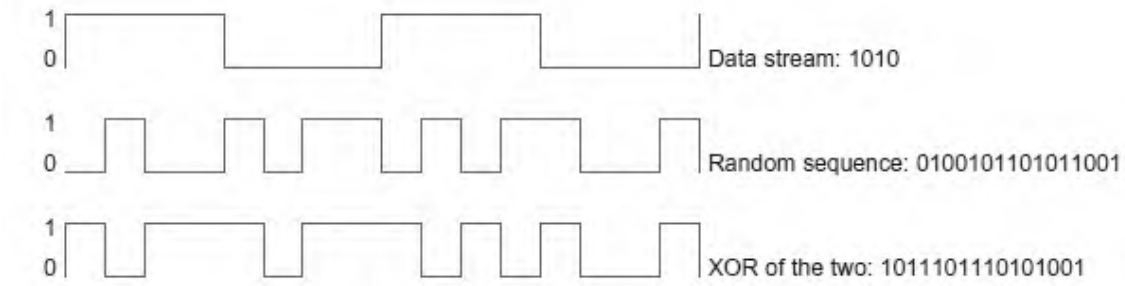
- Frequency hopping is a spread spectrum technique that involves transmitting the signal over a random sequence of frequencies.
- That is, first transmitting at one frequency, then a second, then a third, and so on.
- The random sequence of frequencies is computed by a pseudorandom number generator.

➢ The receiver uses the same algorithm as the sender and initializes it with the same seed and hence is able to hop frequencies in sync with the transmitter to correctly receive the frame.



Direct Sequence Spread Spectrum (DSSS)

➢ Each bit of data is represented by multiple bits in the transmitted signal.
➢ DSSS takes a user data stream and performs an XOR operation with a pseudo – random number.
➢ This pseudo random number is called as ***chipping sequence*****.**



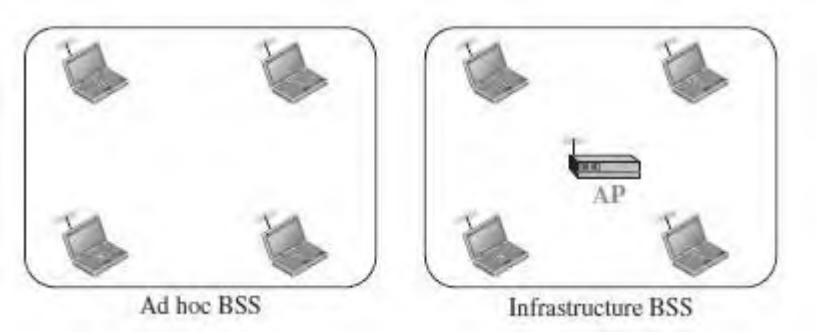
ARCHITECURE OF WLAN / 802.11

- The standard defines two kinds of services: the Basic Service Set (BSS) and the Extended Service Set (ESS).

Basic Service Set (BSS)

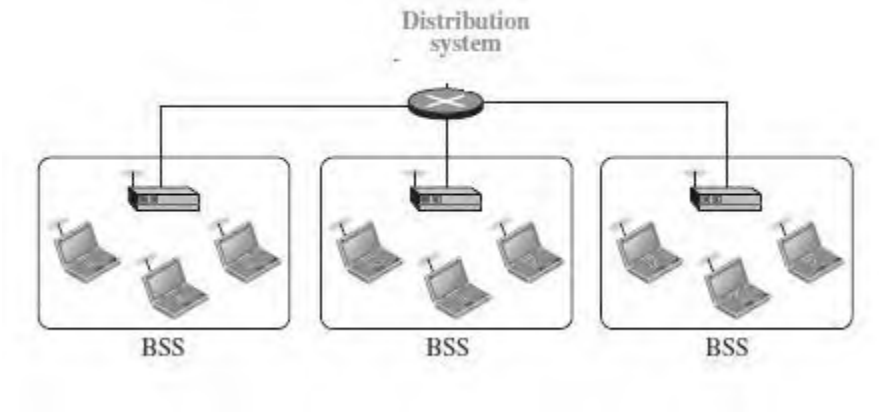
- IEEE 802.11 defines the **basic service set (BSS)** as the building blocks of a wireless LAN.

- A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the *access point (AP)*.



Extended Service Set (ESS)

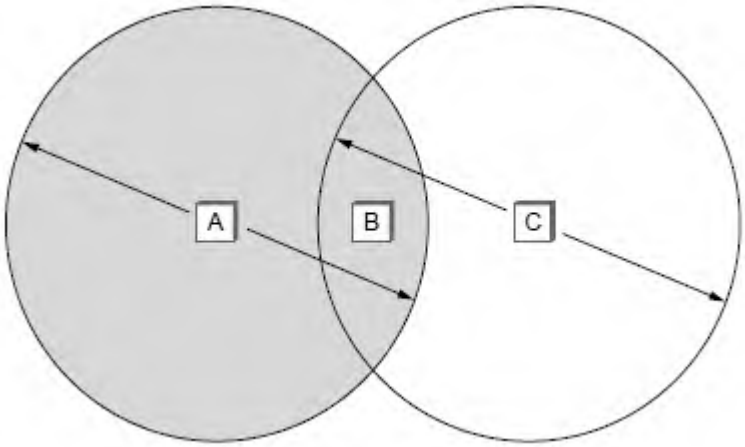
- An extended service set (ESS) is made up of two or more BSSs with APs.
- In this case, the BSSs are connected through a *distribution system*, which is a wired or a wireless network.
- The distribution system connects the APs in the BSSs. The extended service set uses two types of stations: mobile and stationary.
- The mobile stations are normal stations inside a BSS.
- The stationary stations are AP stations that are part of a wired LAN.



COLLISION AVOIDANCE IN WLAN / 802.11

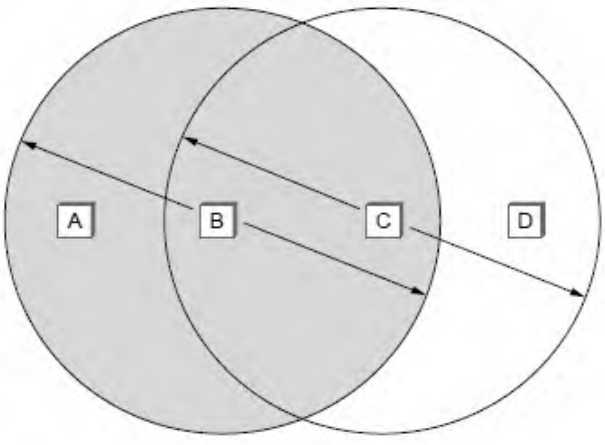
Wireless protocol would follow exactly the same algorithm as the Ethernet—Wait until the link becomes idle before transmitting and back off should a collision occur.

Hidden Node Problem



- Consider the situation shown in the Figure.
- Here A and C are both within range of B but not with each other.
- Suppose both A and C want to communicate with B and so they each send a frame to B.
- A and C are unaware of each other since their signals do not carry that far.
- These two frames collide with each other at B, but neither A nor C is aware of this collision.
- A and C are said to be *hidden nodes* with respect to each other.

Exposed Node Problem



- Each of the four nodes is able to send and receive signals that reach just the nodes to its immediate left and right.
- For example, B can exchange frames with A and C but it cannot reach D, while C can reach B and D but not A.

- Suppose B is sending to A. Node C is aware of this communication because it hears B's transmission.
- If at the same time, C wants to transmit to node D.
- It would be a mistake, however, for C to conclude that it cannot transmit to anyone just because it can hear B's transmission.
- This is not a problem since C's transmission to D will not interfere with A's ability to receive from B.
- This is called exposed problem.
- Although B and C are exposed to each other's signals, there is no interference if B transmits to A while C transmits to D.