***Experiment No- 02B***

***Aim:*** To study about wireless LAN and its architecture.

***Theory:***

A ***wireless local area network*** *(****WLAN****)* is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and yet still be connected to the network. A WLAN can also provide a connection to the wider Internet.

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial complexes that offer wireless access to their customers (often without charge).

Norman Abramson, a professor at the University of Hawaii, developed the world's first wireless computer communication network, ALOHAnet (operational in 1971), using low-cost ham-like radios. The system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines.

Wireless LAN hardware initially cost so much that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (in products using the Wi-Fi brand name). Beginning in 1991, a European alternative known as HiperLAN/1 was pursued by the European Telecommunications Standards Institute (ETSI) with a first version approved in 1996. This was followed by a HiperLAN/2 functional specification with ATM influencesaccomplished February 2000. Neither European standard achieved the commercial success of 802.11, although much of the work on HiperLAN/2 has survived in the physical specification (PHY) for IEEE 802.11a, which is nearly identical to the PHY of HiperLAN/2.

***HiperLAN***

HiperLAN (High Performance Radio LAN) is a Wireless LAN standard.[[1]](https://en.wikipedia.org/wiki/HiperLAN#cite_note-hiperlan-1) It is a European alternative for the IEEE 802.11 standards (the IEEE is an international organization). It is defined by the European Telecommunications Standards Institute (ETSI). In ETSI the standards are defined by the BRAN project (Broadband Radio Access Networks). The HiperLAN standard family has four different versions.

***HiperLAN/1***

Planning for the first version of the standard, called HiperLAN/1, started 1991, when planning of 802.11 was already going on. The goal of the HiperLAN was the high data rate, higher than 802.11. The standard was approved in 1996. The functional specification is EN300652, the rest is in ETS300836.

The standard covers the Physical layer and the Media Access Control part of the Data link layer like 802.11. There is a new sublayer called Channel Access and Control sublayer (CAC). This sublayer deals with the access requests to the channels. The accomplishing of the request is dependent on the usage of the channel and the priority of the request.

CAC layer provides hierarchical independence with Elimination-Yield Non-Preemptive Multiple Access mechanism (EY-NPMA). EY-NPMA codes priority choices and other functions into one variable length radio pulse preceding the packet data. EY-NPMA enables the network to function with few collisions even though there would be a large number of users. Multimedia applications work in HiperLAN because of EY-NPMA priority mechanism. MAC layer defines protocols for routing, security and power saving and provides naturally data transfer to the upper layers.

On the physical layer FSK and GMSK modulations are used in HiperLAN/1.

HiperLAN features:

* slow mobility (1.4 m/s)
* range 50 m
* supports asynchronous and synchronous traffic
* Bit rate - 23.2 Mbit/s
* Description- Wireless Ethernet
* Frequency range- 5 GHz

HiperLAN does not conflict with microwave and other kitchen appliances, which are on 2.4 GHz. An innovative feature of HIPERLAN 1, which may other wireless networks do not offer, is its ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range. For power conservation, a node may set up a specific wake up pattern. This pattern determines at what time the node is ready to receive, so that at other times, the node can turn off its receiver and save energy. These nodes are called p-savers and need so called p-supporters that contain information about wake up patterns of all the p-savers they are responsible for. A p-supporter only forwards data to a p-saver at the moment p-saver is awake. This action also requires buffering mechanisms for packets on p-supporting forwarders.

***HiperLAN/2***

HiperLAN/2 functional specification was accomplished February 2000. Version 2 is designed as a fast wireless connection for many kinds of networks. Those are UMTS backbone network, ATM and IP networks. Also it works as a network at home like HiperLAN/1. HiperLAN/2 uses the 5GHz band and up to 54 Mbit/s data rate

The physical layer of HiperLAN/2 is very similar to IEEE 802.11a wireless local area networks. However, the media access control (the multiple access protocol) is Dynamic TDMA in HiperLAN/2, while CSMA/CA is used in 802.11a/n.

Basic services in HiperLAN/2 are data, sound, and video transmission. The emphasis is in the quality of these services (QoS)

The standard covers Physical, Data Link Control and Convergence layers. Convergence layer takes care of service dependent functionality between DLC and Network layer (OSI 3). Convergence sublayers can be used also on the physical layer to connect IP, ATM or UMTS networks. This feature makes HiperLAN/2 suitable for the wireless connection of various networks.

On the physical layer BPSK, QPSK, 16QAM or 64QAM modulations are used.

HiperLAN/2 offers security measures. The data are secured with DES or Triple DES algorithms. The wireless access point and the wireless terminal can authenticate each other.

Most important worldwide manufacturers of HiperLAN/2 are Alvarion (Israel), Freescale (USA), Panasonic (Japan).

***Types of wireless LAN’s:***

The IEEE 802.11 has two basic modes of operation: ***infrastructure*** and ***ad hoc*** mode. In *ad hoc* mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN).

Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms: Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network.

### ***Infrastructure***

Most Wi-Fi networks are deployed in infrastructure mode. In infrastructure mode, a base station acts as a wireless access point hub, and nodes communicate through the hub. The hub usually, but not always, has a wired or fiber network connection, and may have permanent wireless connections to other nodes.

Wireless access points are usually fixed, and provide service to their client nodes within range. Wireless clients, such as laptops, smartphones etc. connect to the access point to join the network.

Sometimes a network will have a multiple access points, with the same 'SSID' and security arrangement. In that case connecting to any access point on that network joins the client to the network. In that case, the client software will try to choose the access point to try to give the best service, such as the access point with the strongest signal.

### ***Peer-to-peer***

An ad hoc network (not the same as a WiFi Direct network) is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

A WiFi Direct network is another type of network where stations communicate peer to peer. In a Wi-Fi P2P group, the group owner operates as an access point and all other devices are clients. There are two main methods to establish a group owner in the Wi-Fi Direct group. In one approach, the user sets up a P2P group owner manually. This method is also known as Autonomous Group Owner (autonomous GO). In the second method, also called negotiation-based group creation, two devices compete based on the group owner intent value. The device with higher intent value becomes a group owner and the second device becomes a client. Group owner intent value can depend on whether the wireless device performs a cross-connection between an infrastructure WLAN service and a P2P group, remaining power in the wireless device, whether the wireless device is already a group owner in another group and/or a received signal strength of the first wireless device.

A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer. IEEE 802.11 defines the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

### ***Bridge***

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

### ***Wireless distribution system***

A Wireless Distribution System enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between "clients" are made using MAC addresses rather than by specifying IP assignments.

All base stations in a Wireless Distribution System must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers. WDS also requires that every base station be configured to forward to others in the system as mentioned above.

WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). It should be noted, however, that throughput in this method is halved for all clients connected wirelessly. When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

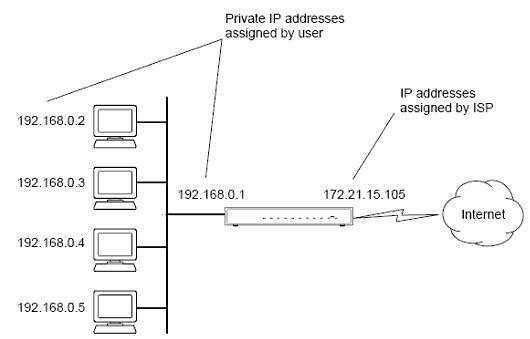
***Wireless LAN Roaming***

There are two types for wireless LAN roaming:

1. **External Roaming:** The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can independently of his home network use another foreign network, if this is open for visitors. There must be special authentication and billing systems for mobile services in a foreign network.
2. **Internal Roaming:** The Mobile Station (MS) moves from one access point (AP) to another AP within a home network because the signal strength is too weak. An authentication server (RADIUS) performs the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data among the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based on proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. The Mobile Station, however, may lose a connection with an access point before associating with another access point. In order to provide reliable connections with applications, the Mobile Station must generally include software that provides session persistence.

***Wireless LAN Architecture***

The process of assembling the parts of computer hardware in computer networking is called as computer architecture. Similarly if we use this architectural technique in Wireless LAN or WiFi is called as Wireless LAN Architecture. It is a technique of designing and arrangement of different components in Wireless local area networking device in a specific way. Special type of device which is the combination of transmitter and receiver called d as transceiver which is an essential part for standard Wireless LAN architecture that is known as Access points.



### ***Components of Wireless Architecture:***

Wireless LAN architecture is composed of different components which help in establishing the local area network between different operating systems. These components are very essential for WiFi architecture.

1. Access point
2. Clients
3. Bridge

***Access Points***

A special type of routing device that is used to transmit the data between wired and wireless networking device is called as AP. It is often connected with the help of wired devices such as Ethernet. It only transmits or transfers the data between wireless LAN and wired network by using infra structure mode of network. One access point can only support a small group of networks and works more efficiently. It is operated less than hundred feet. It is denoted by AP.

***Clients***

Any kind of device such as personal computers, Note books, or any kind of mobile devices which are inter linked with wireless network area referred as a client of wireless LAN architecture.

***Bridge***

A special type of connectors which is used to establish connections between wired network devices such as Ethernet and different wireless networks such as wireless LAN. It is called as bridge. It acts as a point of control in wireless LAN architecture.

Two components are also some time play an important role in Wireless LAN architecture i.e.

1. Basic Service Set (BSS)
2. Extended Service Set (ESS)

***Conclusion:*** Hence we successfully studied wireless LAN its types and its architecture with its components.