WIKIPEDIA

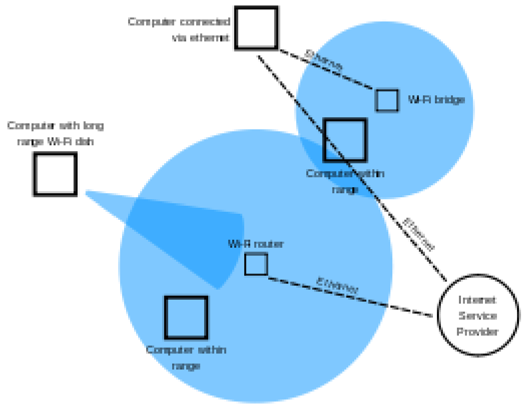
Wireless LAN

A **wireless local area network** (**WLAN**) is a wireless computer network that links two or more devices using wireless communication 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. Through a gateway, a WLAN can also provide a connection to the wider Internet.

This notebook computer is connected to a wireless access point using a PC card wireless card.

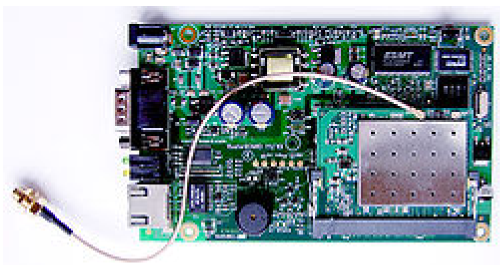
Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name.

Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.



An example of a Wi-Fi network

Contents



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers

History

Norman Abramson, a professor at the University of Hawaii, developed the world's first wireless computer communication network, ALOHAnet. The system became operational in 1971 and included seven computers deployed over four islands to communicate with the central computer on the Oahu island without using phone lines.[1]

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 influences accomplished 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.

54 Mbit/s WLAN PCI Card (802.11g)

In 2009 802.11n was added to 802.11. It operates in both the 2.4 GHz and 5 GHz bands at a maximum data transfer rate of 600 Mbit/s. Most newer routers are able to utilise both wireless bands, known as **dualband**. This allows data communications to avoid the crowded 2.4 GHz band, which is also shared with Bluetooth devices and microwave ovens. The 5 GHz band is also wider than the 2.4 GHz band, with more channels, which permits a greater number of devices to share the space. Not all channels are available in all regions.

A HomeRF group formed in 1997 to promote a technology aimed for residential use, but it disbanded at the end of 2002.[2]

Architecture

Stations

All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or non-portable devices such as desktop computers and workstations that are equipped with a wireless network interface.

Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other at PHY layer. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

Independent basic service set

An IBSS is a set of STAs configured in ad hoc (peer-to-peer)mode.

Extended service set

An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

Distribution system

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use.

Types of wireless LANs

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.

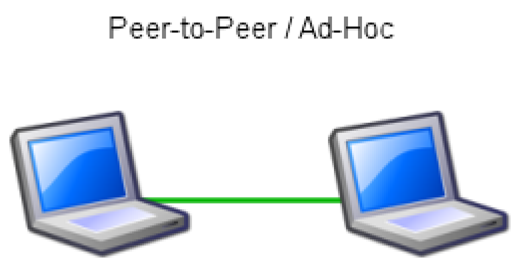
In infrastructure mode, a base station acts as a wireless access point hub, and nodes communicate through the hub. The hub usually, but not always, has a wired or fiber network connection, and may have permanent wireless connections to other nodes.

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



Peer-to-Peer or ad hoc wireless LAN

An ad hoc network (not the same as a WiFi Direct network[3]) 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).

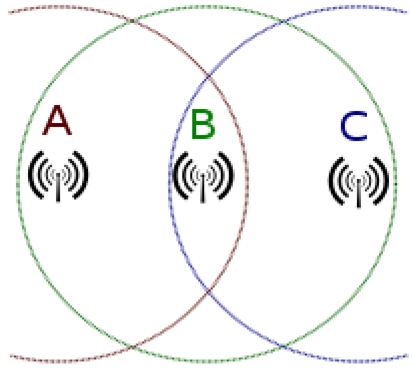
A WiFi Direct network is another type of network where stations communicate peer to peer.

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.



Hidden node problem: Devices A and C are both communicating with B, but are unaware 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 DS over other solutions is that it preserves the MAC addresses of client packets across links between access points.[4]

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.

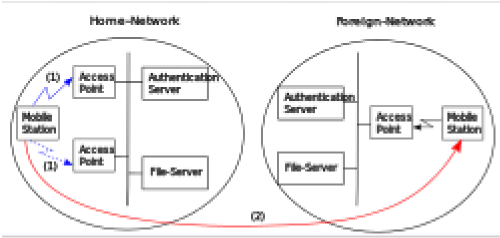
WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). Throughput in this method is halved for all clients connected wirelessly.

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.

Roaming

There are two definitions for wireless LAN roaming:

1. **Internal Roaming:** The Mobile Station (MS) moves from one access point (AP) to another AP within a home network if 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.[5]



Roaming among Wireless Local Area Networks

2. **External Roaming:** The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can use a foreign network independently from their home network, provided that the foreign network allows visiting users on their network. There must be special authentication and billing systems for mobile services in a foreign network.

Applications

Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains.

Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network. Others can be accessed once registration has occurred and/or a fee is paid.

Existing Wireless LAN infrastructures can also be used to work as indoor positioning systems with no modification to the existing hardware.

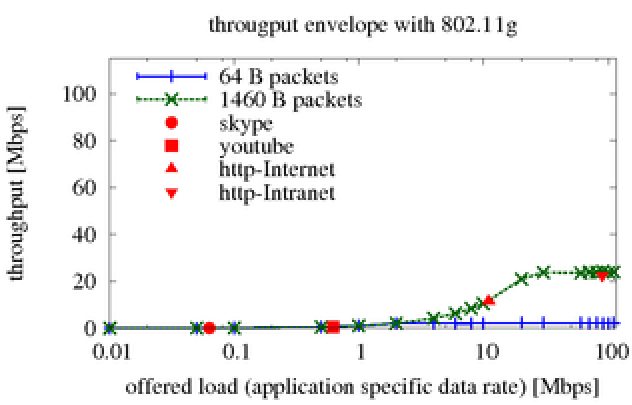
Performance and throughput

WLAN, organised in various layer 2 variants (IEEE 802.11), has different characteristics. Across all flavours of 802.11, maximum achievable throughputs are either given based on measurements under ideal conditions or in the layer 2 data rates. This, however, does not apply to typical deployments in which data are being transferred between two endpoints of which at least one is typically connected to a wired infrastructure and the other endpoint is connected to an infrastructure via a wireless link.

This means that typically data frames pass an 802.11 (WLAN) medium and are being converted to 802.3 (Ethernet) or vice versa.

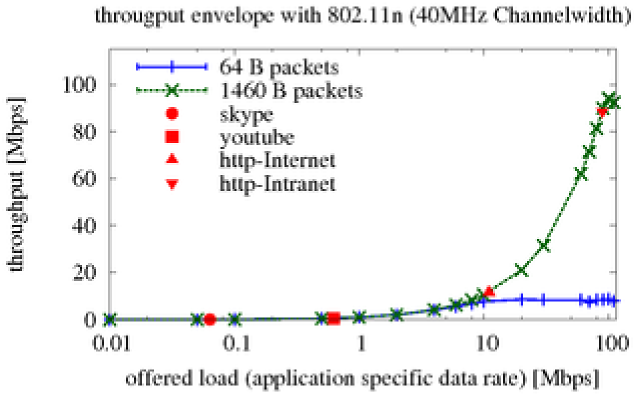
Due to the difference in the frame (header) lengths of these two media, the packet size of an application determines the speed of the data transfer. This means that an application which uses small packets (e.g. VoIP) creates a data flow with a high overhead traffic (e.g. a low goodput).

Other factors which contribute to the overall application data rate are the speed with which the application transmits the packets (i.e. the data rate) and the energy with which the wireless signal is received.



Graphical representation of Wi-Fi application specific (UDP) performance envelope 2.4 GHz band, with 802.11g

The latter is determined by distance and by the configured output power of the communicating devices.[6][7]



Graphical representation of Wi-Fi application specific (UDP) performance envelope 2.4 GHz band, with 802.11n with 40 MHz

Same references apply to the attached throughput graphs which show measurements of UDP throughput measurements. Each represents an average (UDP) throughput (the error bars are there, but barely visible due to the small variation) of 25 measurements.

Each is with a specific packet size (small or large) and with a specific data rate (10 kbit/s – 100 Mbit/s). Markers for traffic profiles of common applications are included as well. This text and measurements do not cover packet errors but information about this can be found at above references. The table below shows the maximum achievable (application specific) UDP throughput in the same scenarios (same references again) with various difference WLAN (802.11) flavours. The measurement hosts have been 25 meters apart from each other; loss is again ignored.

See also

- Local area network
- Wireless WAN
- Wi-Fi

References

1. "History of Wireless" (https://web.archive.org/web/20070210131824/http://www.jhsph.edu/wireless/history.html). *Johns Hopkins Bloomberg School of Public Health*. Archived from the original (http://www.jhsph.edu/wireless/history.html) on 2007-02-10. Retrieved 2007-02-17.
2. Wayne Caswell (November 17, 2010). "HomeRF Archives" (http://www.cazitech.com/HomeRF_Archives.htm). Retrieved July 16, 2011.
3. http://www.wi-fi.org/knowledge-center/faq/same-ad-hoc-mode
4. Wireless Distribution System Linked Router Network (http://www.dd-wrt.com/wiki/index.php?title=WDS_Linked_router_network) *DD-WRT Wiki.* Retrieved December 31, 2006.
5. "How Wi-Fi Roaming Really Works" (http://www.wireless-nets.com/resources/tutorials/how_roaming_works.html). Retrieved 2008-10-09.
6. "Towards Energy-Awareness in Managing Wireless LAN Applications" (https://www.researchgate.net/publication/241631429_Towards_energy-awareness_in_managing_wireless_LAN_applications?ev=prf_pub). IEEE/IFIP NOMS 2012: IEEE/IFIP Network Operations and Management Symposium. Retrieved 2014-08-11.
7. "Application Level Energy and Performance Measurements in a Wireless LAN" (https://www.researchgate.net/publication/224264522_Application_Level_Energy_and_Performance_Measurements_in_a_Wireless_LAN?ev=prf_pub). The 2011 IEEE/ACM International Conference on Green Computing and Communications. Retrieved 2014-08-11.