Wireless Networks

Wireless Standards

As with almost every other aspect of our modern world, regulatory standards regarding wireless use and technologies exist to guide us and act as a reference point for interoperability, efficiency, and other aspects of wireless technologies.

Wireless Standards

Standards are important for several reasons, including the following:

■■ **Interoperability** Standards help to promote interoperability among devices made by different vendors. Individual vendors can build their devices to conform to a particular standard, ensuring that their devices will be able to work together.

■■ **Efficiency** Every vendor can reuse existing solutions that a particular standard has addressed, instead of having to re-create individual solutions.

■■ **Prevention of vendor lock-in** Standards give technology consumers the freedom to choose and buy whatever products they like, which helps to reduce or prevent consumers being locked into solutions provided by particular vendors. When solutions are designed according to standards and specifications, third-party vendors can provide continued support or complementary solutions when an original vendor is no longer able or willing to support its products.

Wireless Standards

IEEE 802.3

The Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard is a collection of IEEE standards that define the properties as well as the working characteristics of the Physical Layer and Data Link Layer's media access control (MAC) sublayer of **wired Ethernet**.

IEEE 802.3 has the feel and functionality that most wireless standards want to emulate, and it is especially concerned with local area network (LAN) technologies, with a nod to some wide area network (WAN) applications since WANs are simply a collection of individual LANs.

Wireless Standards

IEEE 802

The IEEE 802 is not a single standard—it refers to a family of standards. The committee within IEEE that is responsible for this group of standards is known as the IEEE 802 committee, and it deals with LAN, metropolitan area network (MAN), and personal area network (PAN) technologies and standards. It is concerned mostly with the data link and physical layers of the Open Systems Interconnect (OSI) model.

Wireless Standards

IEEE 802.11

The IEEE 802.11 standards comprise various individual standards that cover wireless networking technologies. These standards are forever evolving and adapting to meet technology and industry needs.

The IEEE 802.11 standard specified **data rates of 1 megabit per second (Mbps) and 2 Mbps** and **operated in the 2.4 gigahertz (GHz) band**. All the other IEEE 802.11 standards with letter designations (such as 802.11b) are amendments to this original standard.

Wireless Standards

IEEE 802.11 b

The IEEE 802.11b standard specifies a maximum raw **data rate of 11 Mbit/s**. It was a dramatic improvement in the data rate compared with that offered by the preceding IEEE 802.11 standard (11 Mbit/s vs. 2 Mbit/s). It uses the direct sequence spread spectrum (DSSS)–based modulation scheme.

The standard **specifies operation in the 2.4 GHz band**, which makes WLAN devices subject to interference from a plethora of other everyday devices that operate in the same frequency range (such as microwave ovens and cordless phones).

Wireless Standards

IEEE 802.11 a

The IEEE 802.11a standard **specifies operation in the 5 GHz frequency bands**. It uses the same OFDM (orthogonal frequency division multiplexing) modulation used in IEEE 802.11g. A maximum **data rate of 54 Mbit/s** is specified.

Because 802.11a does not operate in the crowded 2.4 GHz band, it is less prone to interference.

Wireless Standards

IEEE 802.11 g

The IEEE 802.11g standard **specifies operation in the 2.4 GHz** band frequency. The standard specifies a maximum raw **data rate of 54 Mbit/s**. It uses a variant of the OFDM–based modulation scheme as well as the DSSS modulation technique.

Hardware based on the IEEE 802.11g standard is backward-compatible with IEEE 802.11b–based hardware.

Wireless Standards

Wi-Fi

Wi-Fi certification is a process that assures interoperability between 802.11 wireless LAN equipment, including access points and radio cards complying with a variety of form factors.

Wi-Fi certification is meant to give consumers confidence that they are purchasing wireless LAN products that have met multivendor interoperability requirements.

Wi-Fi is short for "**wireless fidelity**"

Wireless Standards

IEEE 802.15

A standard published by the IEEE that defines the radio characteristics and operation of wireless PANs. 802.15 is based on the Bluetooth specification.

Wireless Standards

IEEE 802.16

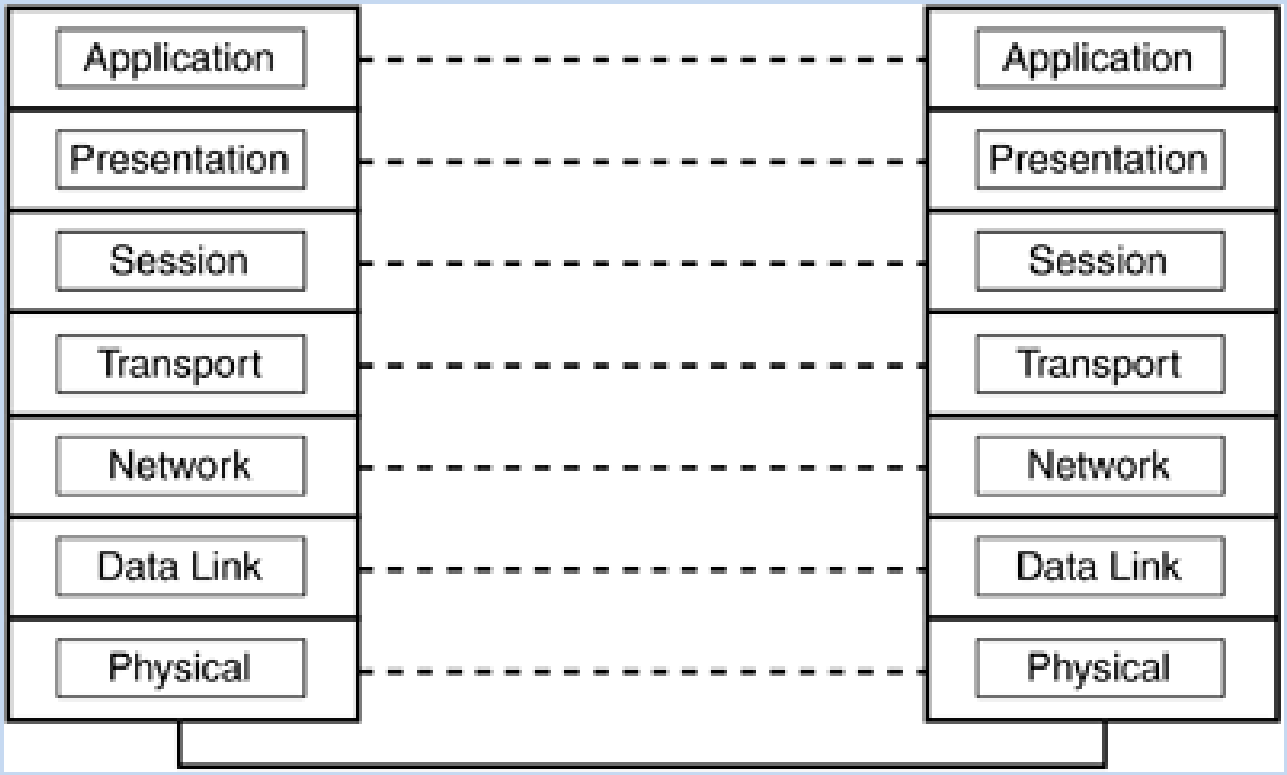
A standard published by the IEEE that defines the radio characteristics and operation of wireless MANs (WiMax).

Network Architecture

The architecture of a network defines the protocols and components necessary to satisfy application requirements. One popular standard for illustrating the architecture is the seven-layer Open System Interconnect (OSI) Reference Model, developed by the International Standards Organization (ISO). OSI specifies a complete set of network functions, grouped into layers which reside within each network component.

Each layer of the OSI model supports the layers above it.

Network Architecture



The OSI Model

Network Architecture

- **Layer 1, Physical layer** defines specifications such as the electrical and mechanical conditions necessary for activating, maintaining, and deactivating the physical link between devices.

- It provides the actual transmission of information through the medium.

- The physical layer is concerned with the binary transmission of data. This binary data is represented as ***bits*** (which is short for *binary digits*). A bit has a single binary value, either 0 or 1.

Network Architecture

- **Layer 2, the Data link layer**, defines the format of data that is to be transmitted across the physical network. It indicates how the physical medium is accessed, including physical addressing, error handling, and flow control.

- The data link layer sends **frames** of data.

- For LANs, the Institute of Electrical and Electronics Engineers (IEEE) split Layer 2 into two sublayers: Logical Link Control (LLC) and Media Access Control (MAC).

- The MAC sublayer specifies the *physical* MAC address that uniquely identifies a device on a network.

Network Architecture

- **Layer 3, Network layer** is responsible for routing, which allows data to be properly forwarded across a logical internetwork (consisting of multiple physical networks).

- The Network layer sends **Packets** of data

- Internet Protocol (IP) addresses (*Logical* network addresses) as opposed to physical MAC addresses are specified at Layer 3.

Network Architecture

- **Layer 4, the Transport layer**, is concerned with end-to-end connections between the source and the destination.
- The Transport layer sends **Segments** of data
- Connection-oriented reliable transport establishes a logical connection and uses sequence numbers to ensure that all data is received at the destination.
- Connectionless best-effort transport just sends the data and relies on upper-layer error detection mechanisms to report and correct problems.
- Reliable transport has more overhead than best-effort transport.

Why?

- Protocols such as Transmission Control Protocol (TCP) operate at this layer.

Network Architecture

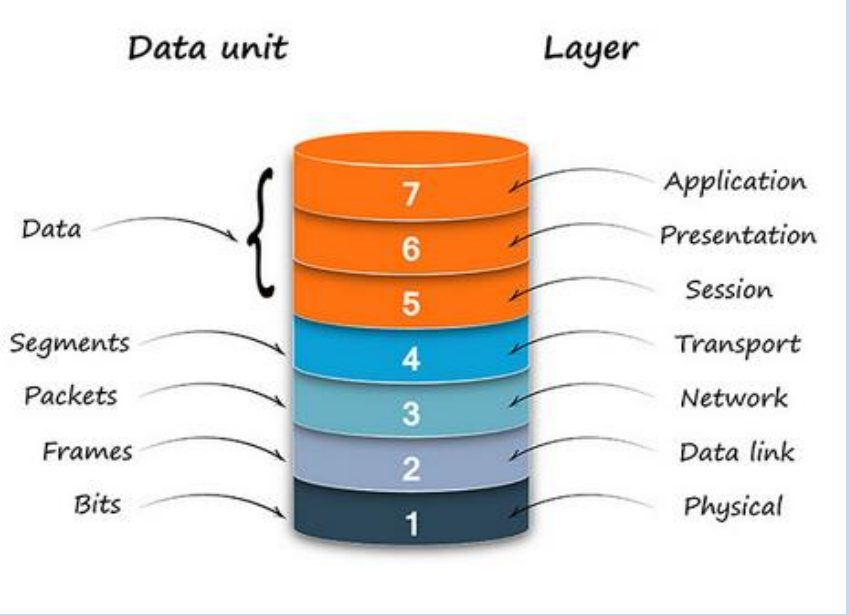
- **Layer 5, the Session layer**, Establishes, manages, and terminates sessions between applications running on different hosts.
- Wireless middleware" software connecting two different and separate applications, e.g. database to web servers" and access controllers provide this form of connectivity over wireless networks. If the wireless network encounters interference, the session layer functions will suspend communications until the interference goes away.

Network Architecture

- **Layer 6, the Presentation layer**, specifies the format, data structure, coding, compression, and other ways of representing the data to ensure that information sent from one host's application layer can be read by the destination host.

Network Architecture

- **Layer 7, the Application layer**, is the closest to the end user; it establishes communications among users and provides basic communications services such as file transfer and e-mail. Examples of software that runs at this layer include Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP) and File Transfer Protocol (FTP).



Network Architecture

- The combined layers of a network architecture define the functionality of a wireless network, but wireless networks directly implement only the two lower layers of the model **(the data link layer and physical layer functions).**

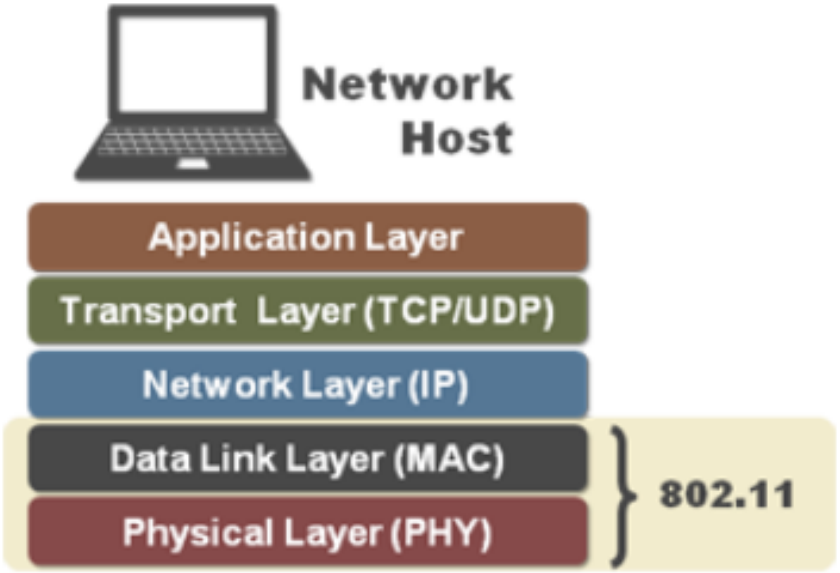
Where does 802.11 fit in the OSI model?

802.11 is a set of *data link* and *physical* layer protocols.

Data Link Layer (MAC):
Responsible for reliable link-to-link data transfer

- Channel access (CSMA/CA)
- Addressing
- Frame Validation (management, data, control frames)
- Error detection
- Security Mechanisms

Physical (PHY) Layer:
Responsible for putting bits "on the air"



Click image to enlarge.

- All Wireless LANs operate on the Physical and Data Link layers, layers 1 and 2. All Wi-Fi systems use these layers to format data and control the data to conform with 802.11 standards.

Wireless Physical layer

- The Physical layer, or PHY, is the medium through which communication is effected. It is at this layer the transceiver is controlled to access the medium.
- Unlike a bounded, wired medium, WLANs operate "over the air" and are subject to an entirely different set of rules for accessing and controlling the medium.
- For instance, wired networks have the ability to detect and mitigate data collisions; wireless networks cannot detect collisions, instead, elaborate protocols are in place to allow access and control of the medium and to avoid collisions.

- Wireless networks are also subject to unintentional interference and intentional disruptions.
- Wired networks are relatively difficult to hack into while wireless networks can be casually hacked by anyone with a wireless card within range of an access point.
- These issues have provided developers with significant challenges to overcome to ensure that WLANs are reliable and secure.

- The Data Link layer consists of two sublayers: the Logical Link Control (LLC) sublayer and the Medium Access Control (MAC) sublayer.
- The LLC receives an IP packet from the Network layer above it and encapsulates the data with addressing and control information. This packet, now called a frame, is passed to the MAC, which modifies the addressing and control information in the frame header to ensure the data is in the proper form for application to the Physical layer.
- The MAC then passes the frame to the PHY, which modulates the data according to the PHY standard.

References

- 1- Wireless Network Administration
- 2- https://www.controleng.com/single-article/wi-fi-and-the-osi-model/8b71b0494b6b7fd5291856d02e104eb4.html