Name	**Khalid**
ID	**15092**
Assignment	**wireless Network**
Submitted to	**Engr Naeem**
Submitted by	**Khalid**

What is wireless network?

A wireless network is a computer network that uses wireless data connections between network nodes. ... Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

OR

Wireless networks are computer networks that are not connected by cables of any kind. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations

How wireless Network work?

A wireless network or Wireless Local Area Network (WLAN) serves the same purpose as a wired one — to link a group of computers.

A wireless network or Wireless Local Area Network (WLAN) serves the same purpose as a wired one — to link a group of computers. Because "wireless" doesn't require costly wiring, the main benefit is that it's generally easier, faster and cheaper to set up.

By comparison, creating a network by pulling wires throughout the walls and ceilings of an office can be labor-intensive and thus expensive. But even when you have a wired network already in place, a wireless network can be a cost-effective way to expand or augment it. In fact, there's

really no such thing as a purely wireless network, because most link back to a wired network at some point.

The Basics

Wireless networks operate using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space.

The cornerstone of a wireless network is a device known as an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. Since wireless networks are usually connected to wired ones, an access point also often serves as a link to the resources available on the a wired network, such as an Internet connection.

In order to connect to an access point and join a wireless network, computers must be equipped with wireless network adapters. These are often built right into the computer, but if not, just about any computer or notebook can be made wireless-capable through the use of an add-on adapter plugged into an empty expansion slot, USB port, or in the case of notebooks, a PC Card slot.

Wireless Technology Standards

Because there are multiple technology standards for wireless networking, it pays to do your homework before buying any equipment. The most common wireless technology standards include the following:

- 802.11b: The first widely used wireless networking technology, known as 802.11b (more commonly called Wi-Fi), first debuted almost a decade ago, but is still in use.
- 802.11g: In 2003, a follow-on version called 802.11g appeared offering greater performance (that is, speed and range) and remains today's most common wireless networking technology.
- 802.11n: Another improved standard called 802.11n is currently under development and is scheduled to be complete in 2009. But even though the 802.11n standard has yet to be finalized, you can still buy products based on the draft 802.11n standard, which you will be able to upgrade later to the final standard.

All of the Wi-Fi variants (802.11b, g and n products) use the same 2.4 GHz radio frequency, and as a result are designed to be compatible with each other, so you can usually use devices based on the different standards within the same wireless network. The catch is that doing so often requires special configuration to accommodate the earlier devices, which in turn can reduce the overall performance of the network. In an ideal scenario you'll want all your wireless devices, the access point and all wireless-capable computers, to be using the same technology standard and to be from the same vendor whenever possible.

Wireless Speed & Range

When you buy a piece of wireless network hardware, it will often quote performance figures (i.e., how fast it can transmit data) based on the type of wireless networking standard it uses, plus any added technological enhancements. In truth, these performance figures are almost always wildly optimistic.

While the official speeds of 802.11b, 802.11g, and 802.11n networks are 11, 54, and 270 megabits per second (Mbps) respectively, these figures represent a scenario that.s simply not attainable in the real world. As a general rule, you should assume that in a best-case scenario you.ll get roughly one-third of the advertised performance.

It's also worth noting that a wireless network is by definition a shared network, so the more computers you have connected to a wireless access point the less data each will be able to send and receive. Just as a wireless network's speed can vary greatly, so too can the range. For example, 802.11b and g officially work over a distance of up to 328 feet indoors or 1,312 feet outdoors, but the key term there is "up to". Chances are you won't see anywhere close to those numbers.

As you might expect, the closer you are to an access point, the stronger the signal and the faster the connection speed. The range and speed you get out of wireless network will also depend on the kind of environment in which it operates. And that brings us to the subject of interference.

Wireless Interference

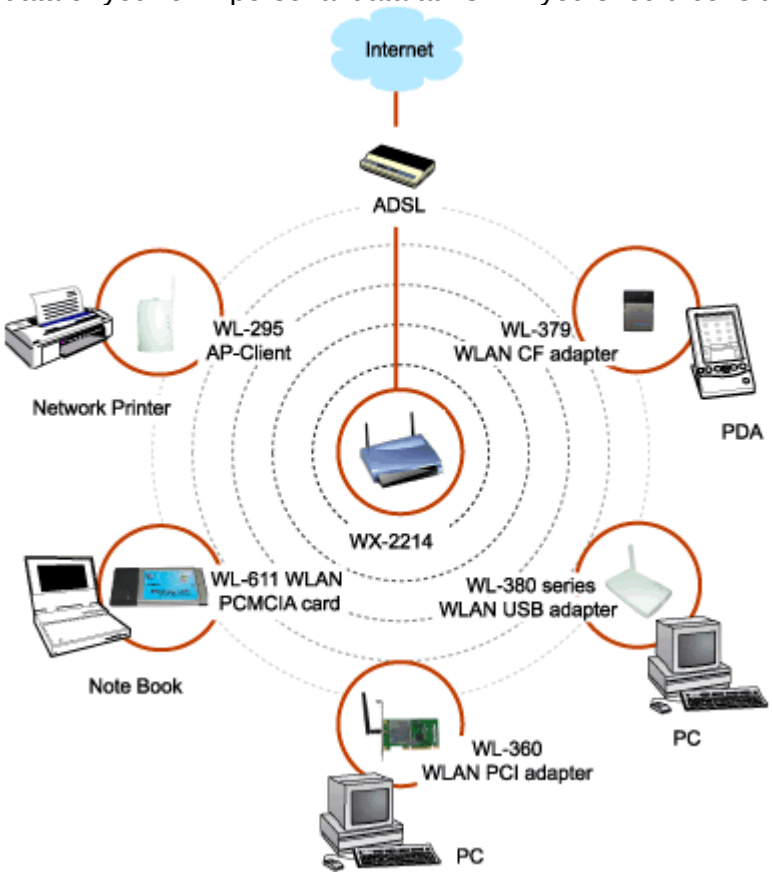
Interference is an issue with any form of radio communication, and a wireless network is no exception. The potential for interference is especially great indoors, where different types of building materials (concrete, wood, drywall, metal, glass and so on) can absorb or reflect radio waves, affecting the strength and consistency of a wireless network's signal. Similarly, devices like microwave ovens and some cordless phones can cause interference because they operate in the same 2.4 frequency range as 802.11b/g/n networks. You can't avoid interference entirely, but in most cases it's not significant enough to affect the usability of the network. When it does, you can usually minimize the interference by relocating wireless networking hardware or using specialized antennas.

Data Security on Wireless Networks

In the same way that all you need to pick up a local radio station is a radio, all anyone needs to detect a wireless network within nearby range is a wireless-equipped computer. There's no way to selectively hide the presence of your network from strangers, but you can prevent

unauthorized people from connecting to it, and you can protect the data traveling across the network from prying eyes. By turning on a wireless network's encryption feature, you can scramble the data and control access to the network.

Wireless network hardware supports several standard encryption schemes, but the most common are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2). WEP is the oldest and least secure method and should be avoided. WPA and WPA2 are good choices, but provide better protection when you use longer and more complex passwords (all devices on a wireless network must use the same kind of encryption and be configured with the same password).
Unless you intend to provide public access to your wireless network — and put your business data or your own personal data at risk — you should consider encryption mandatory.



Invention of wireless network

In 1991, NCR Corporation with AT&T Corporation invented the precursor to 802.11, intended for use in cashier systems. The first wireless products were under the name WaveLAN. They are the ones credited with inventing Wi-Fi. Dr. O'Sullivan is credited with the development of a technology that resulted in wireless LAN becoming reliable and faster. The technology was

instrumental in the invention of **WiFi**, earning Dr. O'Sullivan, and his team of engineers, credit for pioneering the development of Wi-Fi technology The **Full form of WI-FI** is local area wireless technology. **WI-FI** is a wireless networking technology that uses radio waves to provide high-speed network and Internet connections. Introduced in September 1997, the **name Wi-Fi** also stands for Wireless Fidelity as it is synonymous with WLAN (Wireless Local Area Network). **Wi-Fi** is the name of a wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A common misconception is that the term **Wi-Fi** is short for "wireless fidelity," however this is not the case. **Wi-Fi** is simply a trademarked phrase that means IEEE 802.11x. O'Sullivan, and his team of engineers, credit for pioneering the development of Wi-Fi technology. Born in **Australia**, the engineer received his university education at Sydney University. O'Sullivan made his revolutionary invention while working in the Netherlands' Dwingeloo Radio Observatory in 1977.

Types of Wireless Network Explained with Standards

This tutorial explains Wireless Network types (WLANS, WPANS, WMANS and WWANS) and Wireless network terminology (Ad hoc mode, Infrastructure mode, BSS, ESS, BSA, SSID, WEP, EAP, WPA, WPA2, Infrared, Bluetooth, FHSS, DSSS, FHSS, OFDM, MIMO, RF, Omni directional, 802.11g, 802.11a and 802.11h) in detail.

WLANS: Wireless Local Area Networks

WLANS allow users in a local area, such as a university campus or library, to form a network or gain access to the internet. A temporary network can be formed by a small number of users without the need of an access point; given that they do not need access to network resources.

WPANS: Wireless Personal Area Networks

The two current technologies for wireless personal area networks are Infra Red (IR) and Bluetooth (IEEE 802.15). These will allow the connectivity of personal devices within an area of about 30 feet. However, IR requires a direct line of site and the range is less.

WMANS: Wireless Metropolitan Area Networks

This technology allows the connection of multiple networks in a metropolitan area such as different buildings in a city, which can be an alternative or backup to laying copper or fiber cabling.

WWANS: Wireless Wide Area Networks

These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an ISP. These types of systems are referred to as 2G (2nd Generation) systems.

Type	Coverage	Performance	Standards	Applications
Wireless PAN*	Within reach of a person	Moderate	Wireless PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
Wireless LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
Wireless MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed wireless between homes and businesses and the Internet

Wireless WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas