RLMCA206 MOBILE COMPUTING

MODULE – I

Module - I

Basics of Communication Technologies-Mobile Handsets, Wireless Communications, and server Applications-Components of a wireless communication system-Architecture of a Mobile Telecommunication System– Wireless Networking Standards-WLAN Architecture-Bluetooth Technology

*Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi

Module - I

- Mobile Handsets, Wireless Communications, and server Applications
- Components of a wireless communication system
  - Transmitter, receiver, filter, antenna, amplifier, mixers
- Architecture of a Mobile Telecommunication System
- Wireless Networking Standards
  - ITU, IEEE and ISO
  - IEEE 802.11 standards (a,bc,d,e,f…u)

Module – I Cont'd

- WLAN Architecture
  - Components (Access point, bridge, and LAN card)
  - Applications
    - Campus WLANs
    - Streamlining inventory management
    - Providing LAN
    - WLAN connectivity to geographically dispersed computers
  - Advantages of wireless LAN over wired LAN
    - Mobility
    - Simplicity and speedy deployment

- Bluetooth Technology

Wireless networks

- Access computing/communication services, on the move

- Cellular Networks
  - traditional base station infrastructure systems

- Wireless LANs
  - infrastructure as well as ad-hoc networks possible
  - very flexible within the reception area
  - low bandwidth compared to wired networks (1-10 Mbit/s)

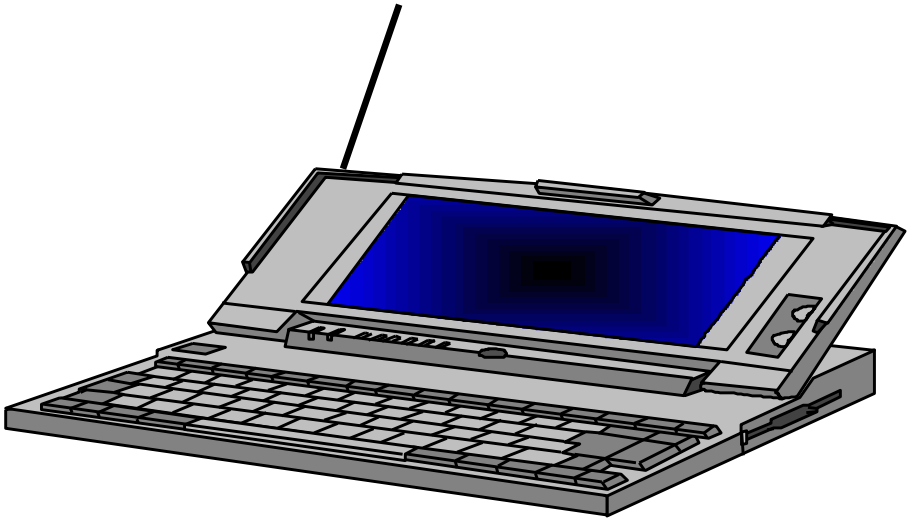
- Ad hoc Networks
  - useful when infrastructure not available, impractical, or expensive
  - military applications, rescue, home networking

Some mobile devices

Palm-sized

Tablets

Clamshell handhelds



Laptop computers

Net–enabled mobile phones

Limitations of the mobile environment

- Limitations of the Wireless Network
  - limited communication bandwidth
  - frequent disconnections

- Limitations Imposed by Mobility
  - route breakages
  - lack of mobility awareness by system/applications

- Limitations of the Mobile Device
  - short battery lifetime
  - limited capacities

Basics of Communication Technologies

- Telecommunications and computer communications that form the essential infrastructure required for building knowledge in the area of mobile computing
- Mobile computing refers to the computational tasks performed by mobile users using their handsets.
- Since the handsets have very limited processing power and memory, these devices by themselves do not have the capability to carry out any significant and meaningful computations and can only serve as the front-end for invoking remote applications.
- Mobile computation, therefore, inevitably involves the invocation of applications running on remote servers.

- Mobile computation is usually achieved by the interaction of a front-end application running on the mobile handset with a server; seamlessly, through the medium of wireless communication.

- Therefore, a study of mobile computation involves the study of the invocation mechanisms at the client end, the underlying wireless communication, and the corresponding server-side technologies.

Mobile Handsets, Wireless Communications, and Server Applications

- Wireless networking has its roots in radio communications.
- In wireless communication, individual users with handsets may directly communicate with each other over a radio link or via several radio and wired links formed through some intermediaries such as base stations and fixed line networks.
- When all the intermediaries are located on the ground, then the communication system is referred to as a *terrestrial radio system.*
- *If at* least one of the intermediaries is satellite borne, then it is referred to as a *satellite radio system.*

- Radio transmission was first discovered by Marconi in the year 1895

- Starting with the elementary, ground-breaking point-to-point wireless communication achieved by Marconi, there has been continually the induction of new and increasingly sophisticated technologies.

- Sophisticated communication techniques such as conventional radio, television, digital packet radio, cellular phone, wireless LAN, and wireless-based Internet access have rapidly been developed over a relatively short span of time.

- These have impacted our daily life, culture, and society in no mean ways. More recently, a technology that has revolutionized the human society and impacted almost everybody, is the *cellular communication technology.*

Cell Phone System

- More than half the world's population today owns cell phones.
- Remarkable acceptance due to their major advantages over the traditional phones.

- Besides providing the flexibility of communicating while on the move, the cell phone system also provides data services such as Short Message Service (SMS), Multimedia Messaging Service (MMS), and even email and web browsing while on the move.

- When the user moves, the current location of the mobile phone is maintained by the network so that any voice call or SMS can be easily sent to the handset wherever it may be.

- This has made it possible for people to communicate and carry out important work anytime and from anywhere.-

Cellular telephony

- Based on radio frequency communications
- A cellular communication system divides the service areas into different geographic zones called *cells*
- Each cell can support a certain maximum number of simultaneous user connections. Consequently, more cells are required per unit area in cities
- Each user has a mobile handset that has its own radio transmitter and receiver antenna to establish connection to the local base station.
- The base station in turn connects to a switching centre.
- The switching centre act as a middleman between two mobile handsets and establishes connections between them when requested.

- As a user moves from one place to another, his call is handled by the switching centre of the base station located in another cell site, thus, providing a consistent high quality signal.

- When a user travels outside his home network, he can still make calls.

- This is possible by a facility called *roaming* and it works because the base station in the local cell is connected by wires with all other networks.

- This makes it possible for a user to get his call almost anywhere.

- If someone dials a user's number, the network finds him and gives him the ring tone.

Components of a wireless communication system

1. Transmitter
2. Receiver
3. Filter
4. Antenna
5. Amplifier
6. Mixers

Components of a Wireless Communication System

1. *Transmitter:*
   - The input to a wireless transmitter may be voice, video, data or other types of signal meant to be transmitted to one or more distant receivers. This signal is called the baseband signal.
   - The basic function of the transmitter is to modulate, or encode several baseband signals onto a high frequency carrier signal.
   - A modulated high frequency signal can be radiated and propagated more effectively and helps make more efficient use of the radio frequency (RF) spectrum than what the direct transmission of the individual baseband signals can achieve.

2. *Receiver:*

- The receiver receives the modulated signals and reverses the functions of the transmitter component and thereby recovers the transmitted baseband signal.

- The antenna of the receiver is usually capable of receiving the electromagnetic waves radiated from many sources

3.Antenna: The function of an antenna is to convert the electric signal from a transmitter to a propagating electromagnetic RF wave; or conversely, to convert a propagating RF wave to an electric signal in a receiver. In a *transceiver,* a transmitter and a receiver are co-located for supporting full-duplex communications. In this case, the same antenna is usually shared by both the transmitter and the receiver. There are mainly two types of antennas that are used on wireless networks:

- omni-directional - can receive and transmit over 360 degrees. This can be compared to a light bulb that emits light all over.
- directional - similar to a flashlight, it focuses light in some direction.

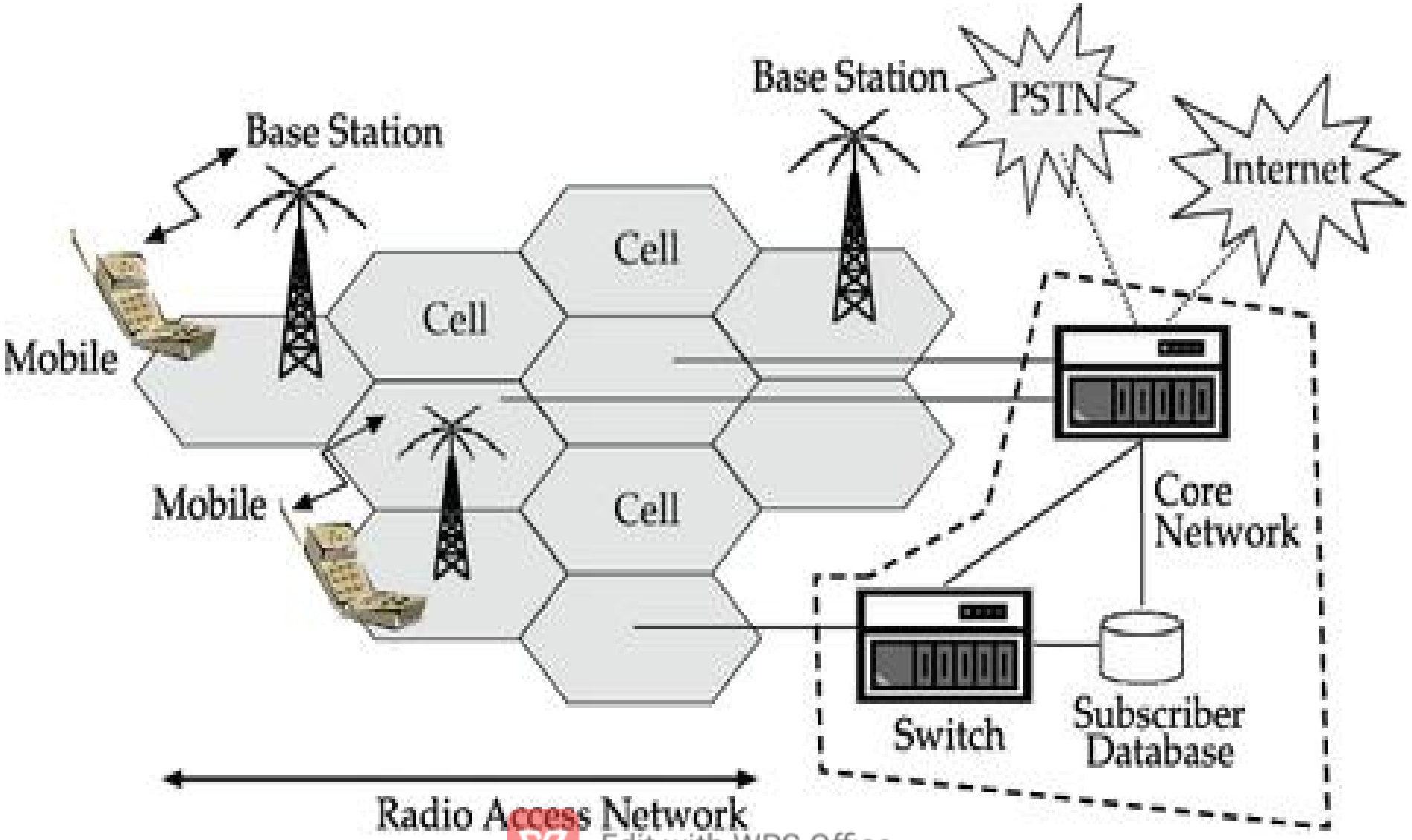
4. *Filters:* Filters are a key component present in all wireless transmitters and receivers. They are used to reject interfering signals lying outside the operating band of receivers and transmitters. They also reject unwanted noise signals generated by the amplifier circuitry.

5. *Amplifiers:* An amplifier amplifies the strength (usually voltage) of a signal. The important specifications of an amplifier include power gain and the noise figure. The noise figure of an amplifier is a measure of how much noise is added to the amplified signal by the amplifier circuitry. This is most critical in the front-end of the receiver where the input signal is very weak and it is desirable to minimize the noise added by the receiver circuitry. Therefore, it is necessary that the first amplifier in the receiver circuit has as low a noise figure as possible.

6. *Mixers*:

- A mixer is typically used to achieve frequency conversion at the transmitters and receivers.
- Frequency conversion is required because it is advantageous to transmit signals at a higher frequency.
- This is achieved by modulating a carrier waveform using the original baseband frequency.
- When a baseband signal is mixed appropriately with a high frequency on a carrier; it can be easily and efficiently radiated and becomes less susceptible to noise and attenuation.
- Therefore, the transmission range increases and the received signal quality improves.
- Further; multiple baseband signals can be mixed with a carrier appropriately in order to efficiently utilize the spectral bandwidth. -modulation technique.
- When multiple baseband signals modulate multiple carrier frequencies and the different baseband signals are made to occupy non-overlapping bandwidths over a frequency spectrum, a *broadband* signal is obtained.

Architecture of a Mobile Telecommunication System



Mobile Telecommunication System

- Three main components:
  - core network
  - radio access network
  - mobile phones.
- Mobile handsets communicate over the radio access network.

- The radio access network is primarily composed of the base stations which communicate with the mobile phones using radio frequency electromagnetic waves.

- Coverage area is decomposed into hexagonal cells.
- In each hexagonal cell, one base station is located.

Mobile Telecommunication System

- Two types of radio channels are usually involved in the communication between a base station and the cell phones:
  - control channels - use frequency shift keying (FSK) and are used for transferring control messages (data) between the mobile phone and the base station.
  - voice channels. - use frequency modulation (FM).

- A base station typically has two antennas of different characteristics. One antenna is used for receiving and the other for transmitting.

- The use of the two different types of antennas at the base station increases the ability of the base station to receive the radio signal from mobiles that use very low transmitter power levels.

- On the other hand, mobile handsets typically use the same antenna for both receiving and transmitting.

- The core network interconnects the base stations, switches the **mobile switching centre (MSC),** and also provides an interface to other networks such as the traditional telephone network (PSTN) and the Internet.

- The interconnect used in the core network is required to provide **high-speed connectivity**.

- Therefore, usually **fiber optic cables** are used as the interconnect in the core network. But based on the terrain conditions, **microwave communication** is also sometimes used.
- This interconnection in the core network must allow **both voice and control information** to be exchanged between the switching system and the base station.

- The MSC is connected to the **landline telephone network** to allow mobile telephones to be connected to standard landline telephones.
- The core network is responsible for transmitting voice calls, SMS (Short Message Service), etc. from one phone to another through switches.
- The core network also maintains a **database** that contains information about **the subscribers and the information about billing**.

Wireless Networking Standards

- Standardization is very important to the computer networking domain since many protocols and devices need to interoperate in any practical networking solution.
- There can be various vendors manufacturing the networking equipment. In the absence of appropriate standards, it would become difficult to interoperate the products manufactured by different vendors.
- Mainly, three international standardization bodies are responsible for formulating the networking standards: ITU, IEEE and ISO.
- The IEEE (Institute of Electrical and Electronics Engineers) is a non-profit, technical professional association of members from over 150 countries. It acts as a standards body.
- Standards are very important in networking since multiple devices that are often heterogoneous and manufactured by different vendors need to communicate.
- The IEEE proposes standards for new technologies and maintains the old standards.
- The IEEE created the 802 group to help standardize the LAN technology.
- The 802.3 standard from this group defines the requirements that a product must meet for it to be considered "Ethernet".

- Wireless Ethernet is defined by 802.11. The 802.11 standard is further broken down into more specific certifications, such as 802.11a, 802.11b, and 802.11g. Each of these defines a different method for providing wireless Ethernet. Each protocol specifies various aspects of data transfer that distinguish them from the other protocols.
- The 802.11 standards define rules for communication on wireless local area networks (WLANs). The popular 802.11 standards include 802.11a. 802.11b and 802.11g. The 802.11 was the original standard in this family, ratified in 1991. It defined WLANs that operated at 1-2 Mbps. This standard is obsolete today, but its extensions are being used extensively.
- Each extension to the original 802.11 appends a unique letter to its name. For example, the standards 802.11a, 802.11b and 802.11g define different types of signal modulation and frequencies of operation as shown in Table 1.1.
- The following IEEE 802 11 standards are being used for wireless local area networking:
- 802.11a: 54 Mbps standard, 5 GHz signalling (ratified 1999)
- 802.11b:11 Mbps standard, 2.4 GHz signalling (1999)

Wireless Networking Standards

TABLE 1.1 Wireless Networking Standards

Standard	*Data rate*	*Information*
IEEE 802.11	Up to 2 Mbps in the 2.4 GHz band	This specification has been extended into 802.11b.
IEEE 802.11a (Wi-Fi)	Up to 54 Mbps in the 5 GHz band	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11 Mbps in the 2.4 GHz band	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4 GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54 Mbps in the 2.4 GHz band	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4 GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.16 (WiMAX)	Specifies WiMAX in the 10 to 66 GHz range	Commonly referred to as WiMAX or less commonly as WirelessMAN or the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs)
IEEE 802.16a (WiMAX)	Added support for the 2 to 11 GHz range	Commonly referred to as WiMAX or less commonly as WirelessMAN or the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs)

HiperLAN/1 (Europe)	Up to 20 Mbps in the 5 GHz band	Only in Europe. HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Does not provide real isochronous services. Relatively expensive to operate and maintain. No guarantee of bandwidth.
HiperLAN/2 (Europe)	Up to 54 Mbps in the 5 GHz band	Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth.
Open Air	Pre-802.11 protocol, using frequency hopping and 0.8 and 1.6 Mbps bit rate	OpenAir is the proprietary protocol from Proxim. All OpenAir products are based on Proxim's module.

Wireless Local Area Networks (WLANs)

- Wireless Local Area Networks (WLANs) provide connectivity between computers over short distances using the wireless medium.
- Typical indoor applications of WLANs may be in educational institutes, office buildings and factories where the required coverage distances are usually restricted to less than a few hundred feet.
- In the absence of obstructions and with the use of suitable antennas, ranges of up to a few kilometres can be obtained.
- Wireless networks are especially useful when it is impossible or expensive to carry out wiring within or across buildings, or when only temporary access is needed between computers.
- WLANs are useful to provide connectivity among portable computers.

History of wireless networks

- Claude Chappe invented the telegraph in 1792 and Alexander Graham Bell first sent voice transmissions over wire in 1876.
- In 1894, near Bologna, Italy, wireless communication was born. Gulielmo Marconi tapped out a message, causing a bell to ring on the other end of the room without using any wire.
- Scientists began searching for ways to broadcast speech using Marconi's wireless.
- In 1906, Reginald Fessenden did it by using amplitude modulation.
- In 1935, the American engineer Edwin Armstrong introduced FM (frequency modulation) radio waves, which used less power and achieved reception of higher quality signals.
- On October 13, 1983, the first call on a commercial cellular system was made in Chicago.

- Most commercial WLAN products use a number of technologies in accordance with the international standards specified by the Institute of Electrical and Electronic Engineers (IEEE)
- These WLANs operate with maximum data rates of up to 54 Mbps, which are much lower than the data rates that can be achieved with the wired Ethernet connections.
- WLANs almost universally use Internet Protocols (such as TCP/IP) for communication between computers.
- These protocols are basically a set of standard rules to facilitate communication between computers.
- The HIPERLAN standard provides for WLAN operation with bit rate up to 20 Mbps.
- WLANs operate in specific frequency ranges depending on the availability of spectrum in specific countries.

WLAN components

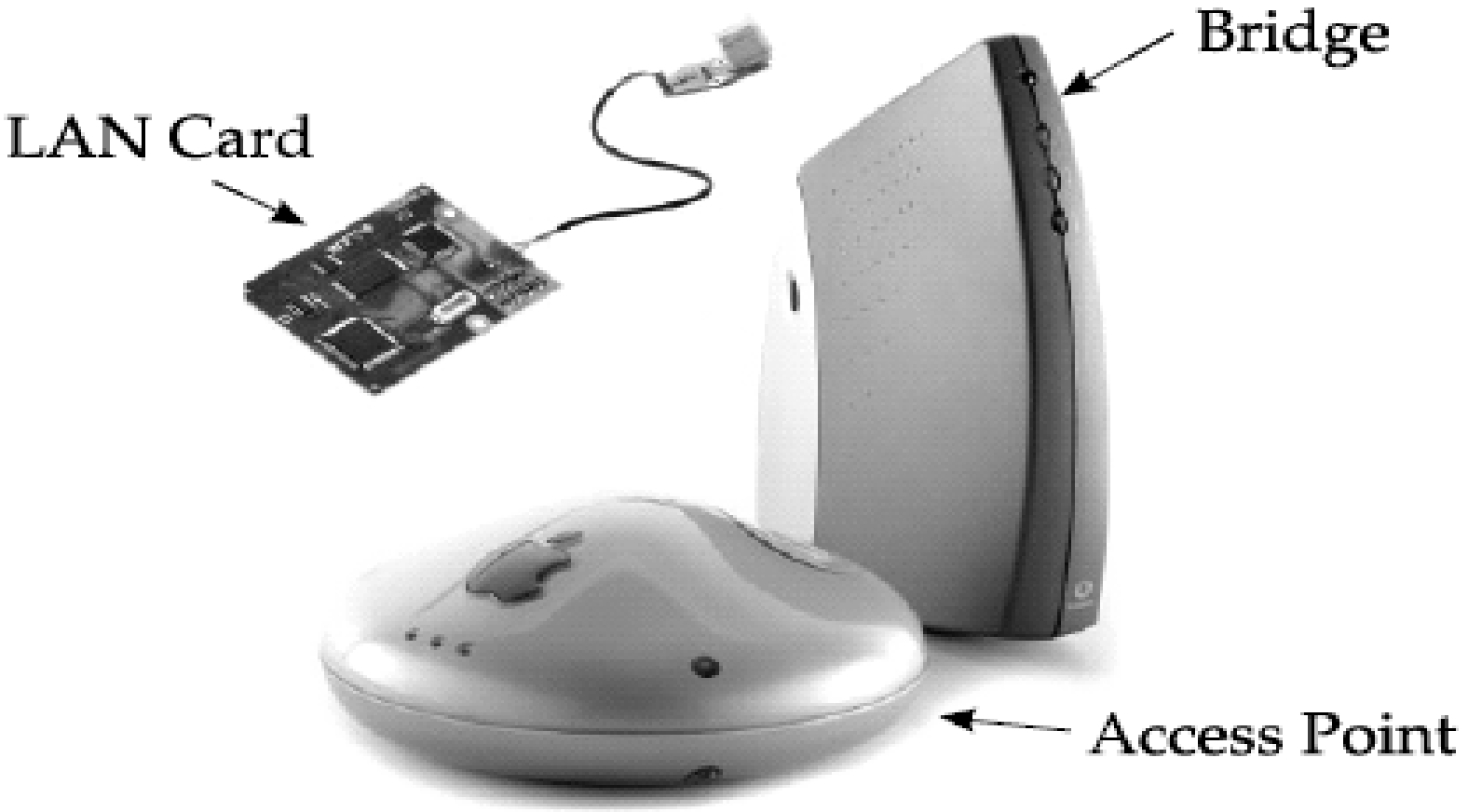


Figure 1.5 *Wireless LAN card, access point and bridge.*

WLAN components

1. ***Access point:***
   - *It is* a radio receiver/transmitter (also called transceiver) that connects to the wired network.
   - These are typically mounted on the roofs at different locations of a building.
   - The transceiver exchanges signals with the wireless LAN card in desktop or notebook PCs.
   - A single access point can support a small group of users.
   - It is connected to a wired network through cables and provides the connectivity between wireless devices and the wired network.

2. ***Wireless LAN cards:***
   - End-users access the WLAN through WLAN adapters (wireless network interface cards) in their hand-helds.
   - The LAN card used to be mounted on the motherboard of a computer. Now, it is inbuilt into the motherboards.

3. ***Bridge:***
   - *It* is used for connecting two LANs that may be in two different buildings or on two separate floors within the same building.

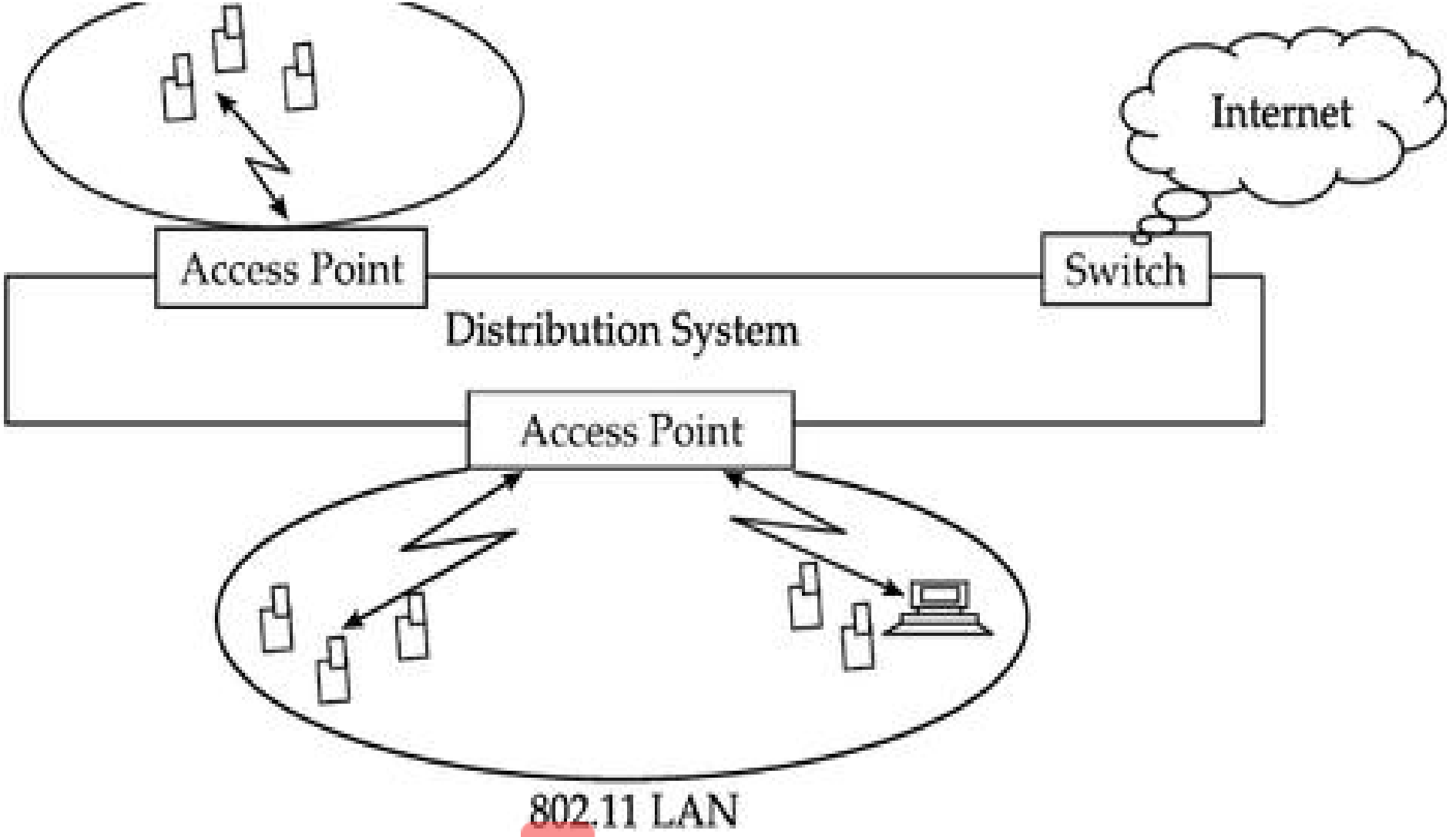
Wireless LAN Architecture

- One access point can provide support to a small group of users and can perform within a range up to a few hundreds of feet.
- The access point (or the antenna attached to the access point) is usually mounted on roof tops but may be mounted elsewhere, if it is practical to do so, as long as the desired radio coverage is obtained.
- End users access the **wireless LAN** through **wireless-LAN adapters**, which are integrated within the hand-held computers.
- Wireless LAN adapters provide an interface between the client's network operating system and the air waves via an antenna.

- One of the main concerns of users of wireless LANs is the apparent reduction in privacy and security.

- To address this issue, WLANs uses multiple levels of security to prevent unauthorized access to network resources.

Architecture of an infrastructure-based IEEE 802.11 network.



- Access points are connected through a distribution system which usually uses a fiber optic cable.
- Mobile nodes are connected to access points.
- The 802.11 standard stipulates that the distribution system may be of any technology, such as Ethernet, token ring, or any other network type.
- The majority of actual installations utilize Ethernet (802.3).
- An 802.3-based distribution system (also referred to as the " wired backbone') consists of switches or hubs that tie together users (PCs and access points) equipped with 802.3 network interface cards (NICs).

- Switch or hub is somewhat analogous to an 802.11 access point.

- The main difference is that a hub or switch provides connection over a physical medium and an access point provides wireless connectivity.

- Two 802.11 LANs are connected via a distribution system.
-
- A distribution system can also be used to increase network coverage through roaming between cells.

- The distribution system also provides connectivity to the Internet through a switch.

Applications of Wireless LANs

1. *Campus wireless LANs:*
   - Several organizations, hotels, retail outlets, warehouses, factories, research centers and educational institutions
   - Users with laptops, PDAs, palmtops can have access to the organization's intranet and to the Internet from any location in the campus.
   - An effective way to make the network-based services available to them is by creating a wireless network.

2. *Streamlining* inventory *management:*

- Stock control and management are the important activities in almost every manufacturing organization and retail outlet.
- Traditionally, manual stockkeeping -stockkeeper going around the godown and noting down the stock levels, counting various item and tallying them manually for inventory control.
- Human errors
- With wireless LAN devices such as hand-held scanners, keypads and bar code readers can be linked to database applications and printers.
- inventory management becomes automatic making stock and inventory control more manageable.

3. *Providing LAN facilities in difficult-to-wire areas:-* Wireless LANs can coexist with wired LANs and help in extending LAN connectivity to locations where providing wired connections is difficult.

4. WLAN *connectivity to geographically dispersed computers:-* Networks of wireless LANs are being used for providing high bandwidth links to connect different branches of an organization spread over a city. These links between WLANs are being set up as Metropolitan Area Networks

Advantages of Wireless LANs over Wired LANs

1. *Mobility:* Wireless LAN systems can help users get information at any place in their organization.
2. *Simplicity and speedy deployment:* The installation procedure of a wireless LAN system is simple because it eliminates the need to run wires through walls. A wireless LAN facility can be set up in an area in a matter of few hours.

3. *Flexibility:* Wireless technology allows the network to be accessible where wiring is difficult to lay. Eg: airport lounge.

4. *Cost effectiveness:* While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware. but in the long run the cost benefits of WLAN are reasonable because of the environment which often requires frequent movements and dynamic changes.

Bluetooth Technology

- The Bluetooth technology has become a popular means to implement a Personal Area Network (PAN). A PAN helps to interconnect a set of computerized devices that an individual person might require. For example, a PAN makes it possible to network various appliances used in daily life such as a microwave oven, fridge, air conditioner mobile phones, etc. This connectivity makes some meaningful applications to become possible. For example, the fridge might automatically send the list of items that are out of stock to the mobile, which can remind a housewife when shopping in the mall. In the present standard, using wireless PAN, a dynamic group of less than 255 devices can be made to communicate within an area of less than 10 metres in diameter Box…

- A prominent advantage of Bluetooth is that it can be used to get rid of the mesh of wires that are required for interconnecting various devices that are positioned near each other For example, the mouse, the camera, the printer etc. can all communicate with the computer using Bluetooth connectivity, making it possible to get rid of the mesh of wires. Such a Bluetooth connectivity among a set of devices is caned *a piconet.* A piconet is essentially a very small (pico means very small) network as Illustrated in Fig. 1.7.

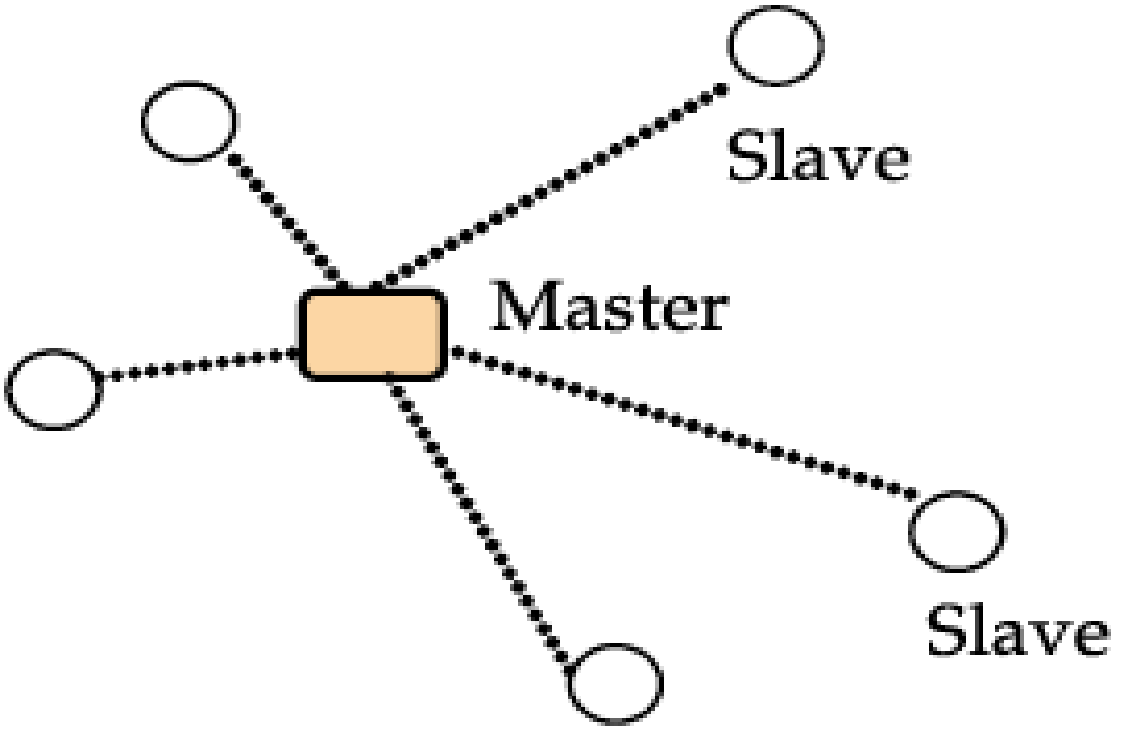


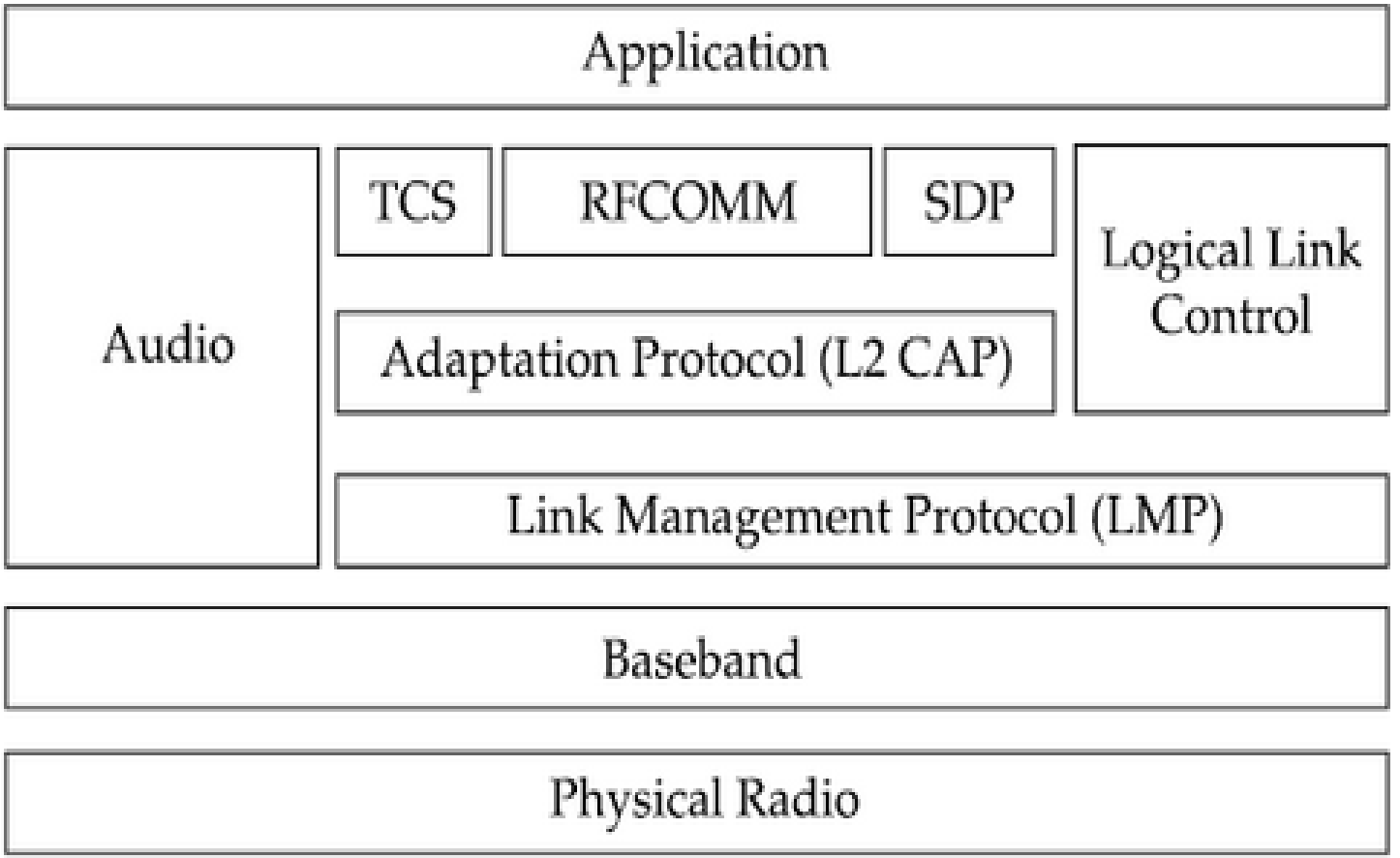
Figure 1.7 *A Bluetooth piconet.*

- A Bluetooth piconet is based on a master-slave communication architecture. One of the computer-enabled devices is designated as the master and the other devices become the slaves. In a piconet, one master device can interconnect with up to seven active slave devices using Bluetooth to form an ad hoc networlc. In Bluetooth communication, the slave units only respond to commands from the master This allows the Bluetooth MAC to be simple, efficient, and non-contention based. In a piconet, data transfer rates of up to 2.1 Mbits are possible. A *scatternet* is formed when an ad hoc network of more than one piconets is fanned.

Protocol Stack of Bluetooth

- Bluetooth protocol stack makes possible the communication of both data and control among many devices in a PAN. The protocol stack is schematically presented in Fig. 1.8.

Bluetooth protocol stock.



- The lowermost layer is called the Radio Frequency (RF) layer. Radio modem is specified in this layer.
- This link controls the packet but the bit levels are specified by the baseband layer.
- The Link Management Protocol (LMP) is capable of configuring links with other devices. It provides power modes, traffic scheduling, packet format, authentication and encryption.
- Logical Link Control and Adaptation Protocol (L2CAP) provide connection-oriented and connectionless data services to the upper layers of the protocol stack.
- Control information may also be exchanged through it.
- L2CAP may include services such as segmentation and re-assembly of data packets.
- The Service Discovery Protocol (SDP) enables two or more Bluetooth devices to support a particular service.

- ***Services Discovery Protocol (SDP):*** Each Bluetooth device maintains an SDP server application that keeps track of the services available on that device. By using this protocol, a mobile application can discover which services are available on which device and can also determine the characteristics of those available services. Thus, it becomes possible to establish connection between two or more Bluetooth devices for specific services. By using SDP, mobile applications can get information such as (I) device information, (II) services, and (iii) service characteristics.

- ***Radio Frequency Communication (RFCOMM):*** RFCOMM is a simple set of transport protocols that are built on top of L2CAP, and helps realize TCP/IP connectivity. It also provides an emulated RS-232 serial port with other Bluetooth devices, thus simplifying connectivity with many simple and small devices without using wires.

- ***Telephony Control Protocol Specification RCS)*** *:* TCS defines the call control signals for establishing a voice connection between Bluetooth devices. This protocol also considers the mobility related issues of hand-held devices. In order to avoid confusion with the popular transport layer protocol, i.e., the Transmission Control Protocol (TCP), this telephone control protocol specification is usually denoted by the abbreviation TCS.

Bluetooth 4.0: Low Energy

How much energy does traditional Bluetooth use?

- Traditional Bluetooth is *connection oriented*. When a device is connected, a link is maintained, even if there is no data flowing.
- Sniff modes allow devices to sleep, reducing power consumption to give months of battery life
- Peak transmit current is typically around 25mA
- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for coin cells and energy harvesting applications

What is Bluetooth Low Energy?

- Bluetooth low energy is a NEW, open, short range radio technology
  - Different to Bluetooth classic (BR/EDR)
  - Optimized for ultra low power
  - Enable coin cell battery use cases
    - < 20mA peak current
    - < 5 uA average current

Basic Concepts of Bluetooth 4.0

- Everything is optimized for lowest power consumption
  - Short packets reduce TX peak current
  - Short packets reduce RX time
  - Less RF channels to improve discovery and connection time
  - Simple state machine
  - Single protocol
  - Etc.

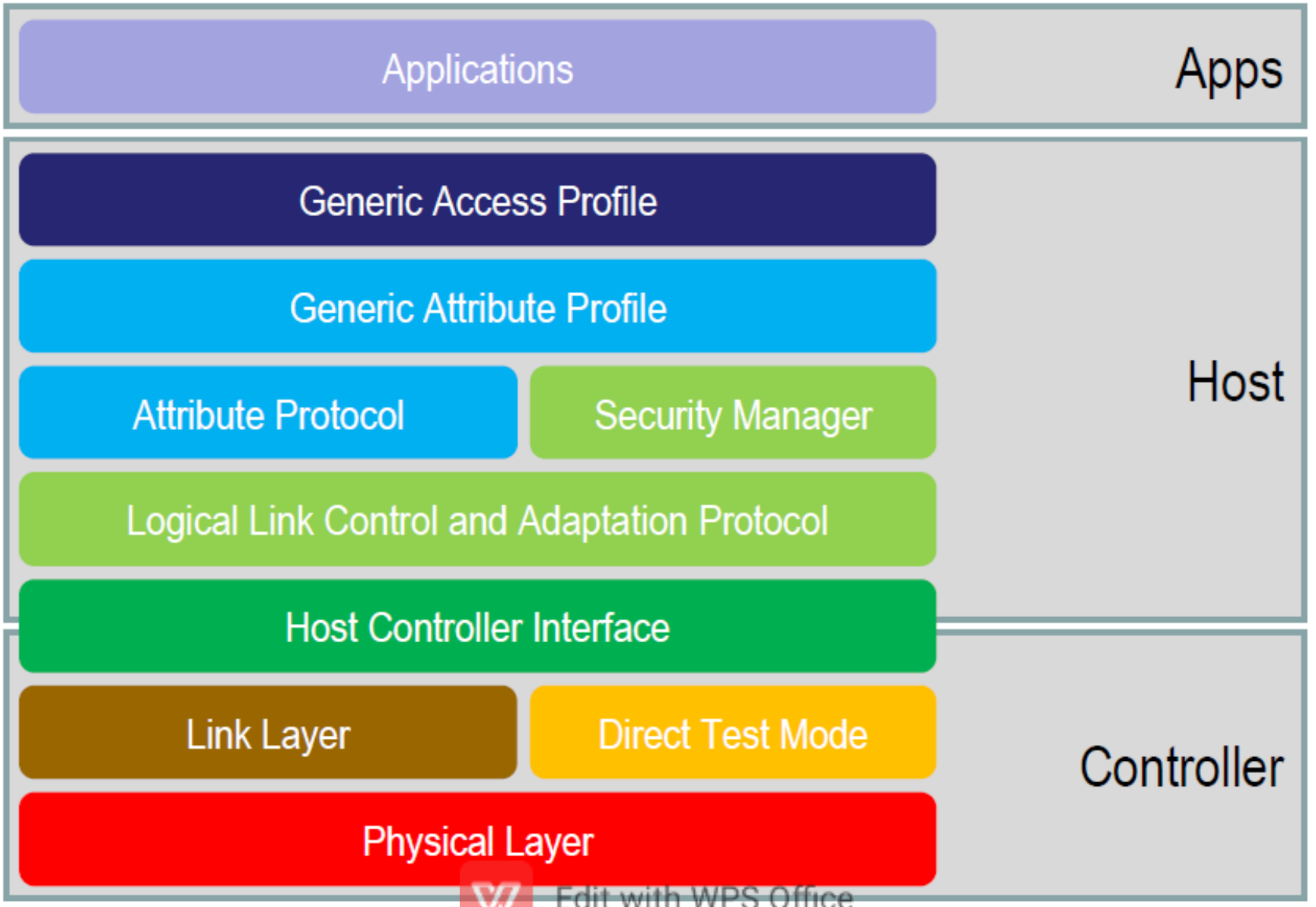
Bluetooth low energy factsheet

Range:	~ 150 meters open field
Output Power:	~ 10 mW (10dBm)
Max Current:	~ 15 mA
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current:	~ 1µA
Modes:	Broadcast, Connection, Event Data Models, Reads, Writes

Bluetooth low energy factsheet #2

- Data Throughput
  - For Bluetooth low energy, data throughput is not a meaningful parameter.
  - It has a data rate of 1Mbps, but is not optimized for file transfer.
  - It is designed for sending small chunks of data

Bluetooth Low Energy Architecture



Device Modes

- Dual Mode
  - Bluetooth BR/EDR and LE
  - Used anywhere that BR/EDR is used today

- Single Mode
  - Implements only Bluetooth low energy
  - Will be used in new devices / applications

Generic Access Profile (GAP)

- Defines the generic procedures related to discovery of Bluetooth devices and link management aspects of connecting to Bluetooth devices
- The Generic Access Profile defines the following roles when operating over the physical channel:
  - Broadcaster role: A device that send advertising events. It is referred to as a Broadcaster. It has a transmitter and may have a receiver.
  - Observer role: device that receives advertising events- Observer. It has a receiver and may have a transmitter.
  - Peripheral role: A device that accepts the establishment of an LE physical link using any of the connection establishment procedures is termed to be in a "Peripheral role." -"Slave role" .A Peripheral has both a transmitter and a receiver.
  - Central role: A device that supports the Central role initiates the establishment of a physical connection. -"Master role" in the Link Layer Connection. A device operating in the Central role is referred to as a Central. A Central has a transmitter and a receiver.

Generic Attribute Profile (GATT)

- Defines a generic service framework using the ATT protocol layer. This framework defines the procedures and formats of services and their Characteristics.
- GATT Roles
  - GATT Client: This is the device that wants data. It initiates commands and requests towards the GATT Server. It can receive responses, indications, and notifications data sent by the GATT Server.
  - GATT Server: This is the device that has the data and accepts incoming commands and requests from the GATT Client and sends responses, indications, and notifications to a GATT Client.

Attribute Protocol (ATT)

- Defines a Client/Server architecture above the BLE logical transport channel.

- The attribute protocol allows a device referred to as the GATT Server to expose a set of attributes and their associated values to a peer device referred to as the GATT Client.

- These attributes exposed by the GATT Server can be discovered, read, and written by a GATT Client, and can be indicated and notified by the GATT Server

Security Manager Protocol (SMP)

- Defines the procedures and behaviour to manage pairing, authentication, and encryption between the devices.
- These include:
  - Encryption and Authentication
  - Pairing and Bonding
    - Pass Key and Out of band bonding
  - Key Generation for a device identity resolution, data signing and encryption
  - Pairing method selection based on the IO capability of the GAP central and GAP peripheral device

Logical Link Control Adaptation Protocol (L2CAP)

- L2CAP provides a connectionless data channel.
- LE L2CAP provides the following features:
  - Channel multiplexing, which manages three fixed channels. Two channels are dedicated for higher protocol layers like ATT, SMP. One channel is used for the LE-L2CAP protocol signalling channel for its own use.
  - Segmentation and reassembly of packets whose size is up to the BLE Controller managed maximum packet size.

Host Controller Interface (HCI)

- The HCI layer implements a command, event, and data interface to allow link layer access from upper layers such as GAP, L2CAP, and SMP.

Link Layer (LL)

- The LL protocol manages the physical BLE connections between devices.
- It supports all LL states such as Advertising, Scanning, Initiating, and Connecting (Master and Slave).
- It implements all the key link control procedures such as LE Encryption, LE Connection Update, LE Channel Update, and LE Ping.
- The Link Layer is a hardware-firmware co-implementation,
- The LL firmware maintains and controls the key LL procedure state machines.
- It supports all the BLE chip specific low power modes.

Physical Layer

- It handles transmission and receiving of bit data.
- It perform modulation and demodulation operations
- Same as that in TCP/IP

NEAR FIELD COMMUNICATION

WHAT IS NFC???

- NFC or Near Field Communication is a short range high frequency wireless communication technology.
- A radio communication is established by touching the two phones or keeping them in a proximity of a few centimeters.
- NFC is mainly aimed for mobile or handheld devices.
- NFC is an extension of Radio frequency identification or RFID technology.
- RFID is mainly used for tracking and identification by sending radio waves.

EVOLUTION OF NFC TECHNOLOGY

- In 2004, NFC Forum was formed by Nokia, Philips, Sony,to set standards for NFC . Every NFC enabled device will have “N-Mark” trademark ,developed by NFC Forum.

N MARK
TRADEMARK

EVOLUTION OF NFC TECHNOLOGY

- In 2006

First mobile phone(nokia 6131) with NFC released by NOKIA.

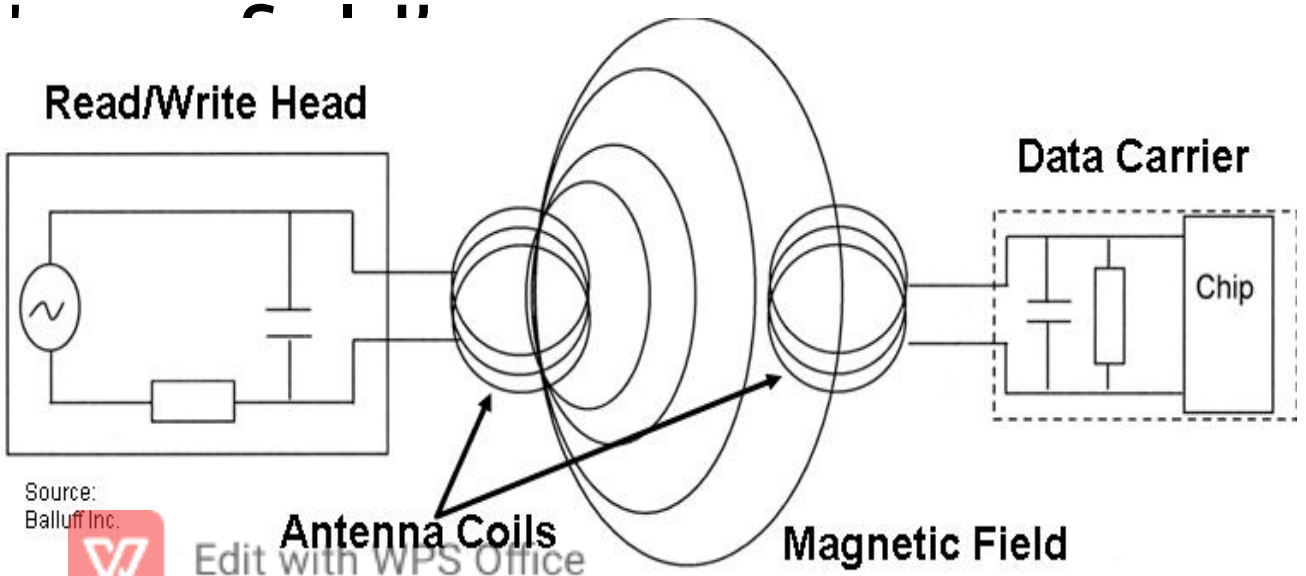
EVOLUTION OF NFC TECHNOLOGY

- In 2010

First android phone SAMSUNG NEXUS S with NFC support released.

OPERATION OF NFC

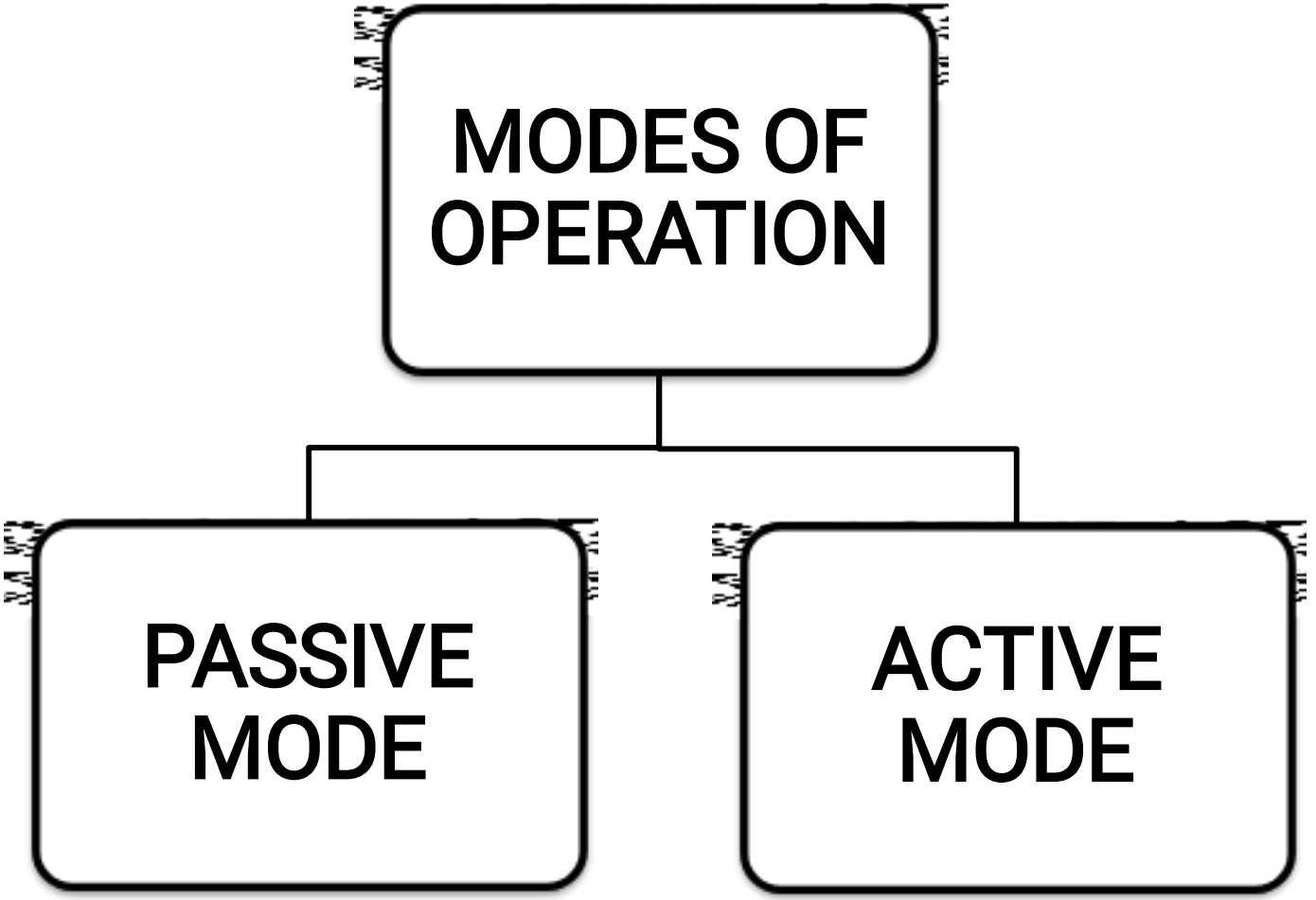
- Near field communication is based on inductive-coupling.
- NFC works using magnetic induction between two loop antennas located within each other's



OPERATION OF NFC

- Operating frequency 13.56MHz.
- Data rate 106 kbit/s to 424 kbit/s.
- NFC use an initiator and a target; the initiator actively generates an RF field that can power a passive tar

MODES OF OPERTAION



MODES OF OPERATION

- In Active mode, both devices with NFC chip generates an electromagnetic field and exchange data.

Two NFC enabled devices transfer-ring data in active mode

MODES OF OPERATION

- In Passive mode, there is only one active device and the other uses that field to exchange information.

A NFC-enabled mobile phone is paired with a RFID-tagged " smart poster"

APPLICATION OF NFC

- NFC applications can be split into the following three basic categories:

➤ Touch and Go
➤ Touch and Confirm
➤ Touch and Connect

APPLICATION OF NFC

- **Touch and Go**

  Applications such as access control or transport/event ticketing, where the user needs only to bring the device storing the ticket or access code close to the reader. Example for picking up an Internet URL from a smart

Touch and go Mode of application

APPLICATION OF NFC

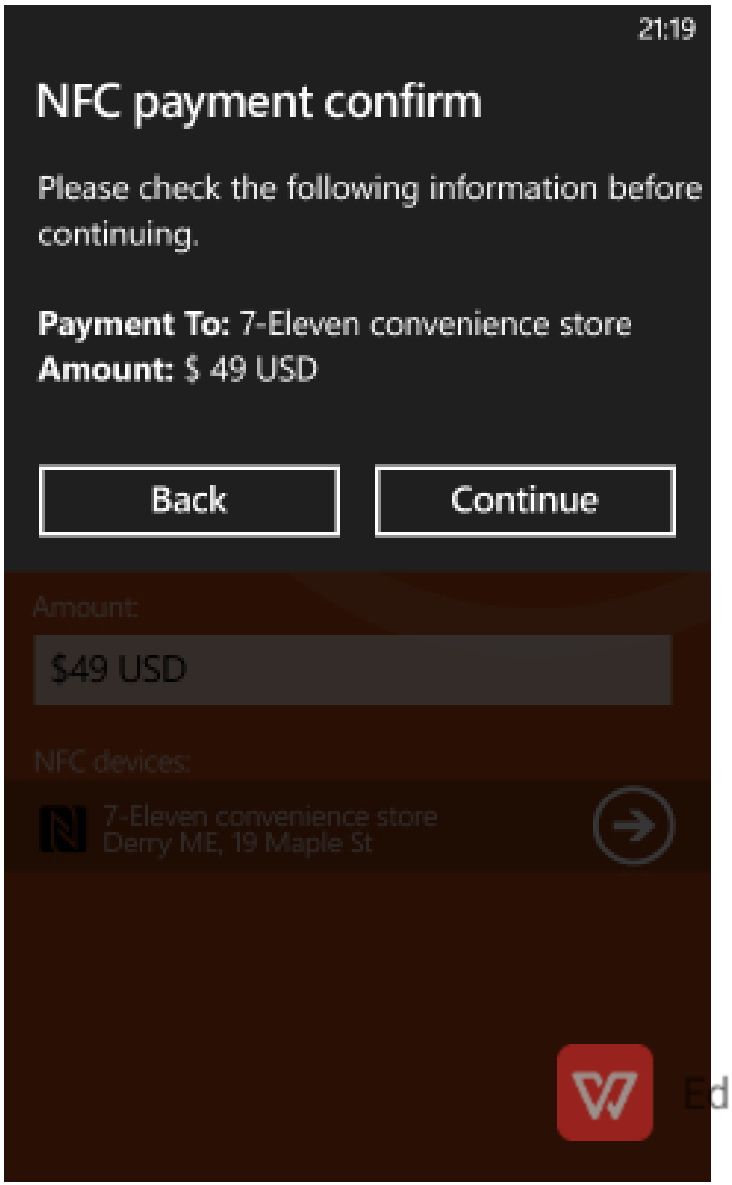
Movie buff gathering info about a movie using his NFC enabled Mobile Phone

APPLICATION OF NFC

- **Touch and Confirm**

Applications such as mobile payment where the user has to confirm the interaction by entering a password or just accepting the transaction.

APPLICATION OF NFC



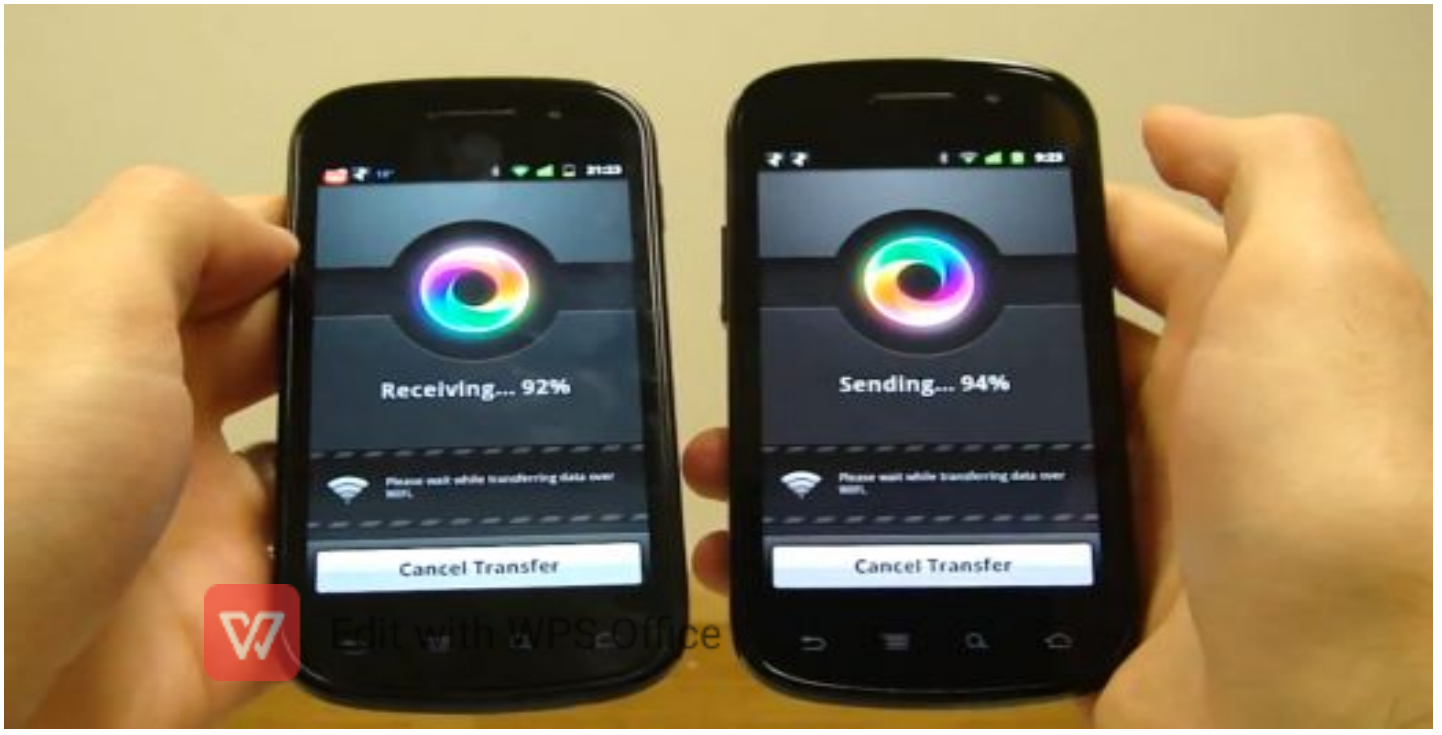
The screenshot from a mobile device showing the confirmation message.

APPLICATION OF NFC

- **Touch and Connect**

Linking two NFC-enabled devices to enable peer to peer transfer of data such as downloading music, exchanging images or synchronizing address books.

Data transfer via NFC



COMPARISON WITH EXISTING TECHNOLOGY

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

ADVANTAGES OF NFC

- High convenience to the user, because the data exchange is done by bringing two mobiles together.
- Reduces cost of electronic issuance .
- Secure communication.
- No special software.
- No manual configuration and settings.
- No search and pair procedure.

DISADVANTAGES OF NFC

- The system has the limitation that it can be operated only with devices under a short range i.e around 10 cm.
- The data transfer rate is very less at about 106kbps, 212 kbps and 424kbps.

SOME DEVICES USING NFC TECHNOLOGY

- Nexus S
- Google Nexus S 4G
- Samsung Galaxy S II
- Samsung Galaxy Note
- Galaxy Nexus
- Nokia 6212 Classic
- Nokia 6131 NFC

DEVICES WITH NFC TECHNOLOGY

FUTURE OF NFC

- New generations of iPhone, iPod and iPad products would reportedly be equipped with NFC capability which would enable small-scale monetary transactions.
- On May 2, 2011, RIM announced the Blackberry Bold 9900, a new device that will use NFC technology.
- Recently, Microsoft announced that all Windows Phone 8 devices will make use of the NFC technology.

CONCLUSION

- Mobile handsets are the primary target for NFC and soon NFC will be implemented in most handheld devices. Even though NFC have the shortest range among radio frequency technologies, combining them with existing technologies like Bluetooth or Infrared can increase its range of applications.

THANK YOU