IT1452 – FUNDAMENTALS OF PERVASIVE

COMPUTING

Prepared by

R.Arivumalar,

Dept of CSE

P.R.Engineering College

Vallam Thanjavur

IT1452 – FUNDAMENTALS OF PERVASIVE COMPUTING

UNIT I PERVASIVE ARCHITECTURE

Local area networks – Wireless LANS – Relationship of wireless, internet and ubiquitous computing – Pervasive computing and ubiquitous computing – Ambient computing – Pervasive web application architecture – Requirements of computational infrastructure – Failure management – Security – Performance – Dependability.

UNIT II MOBILE DEVICE TECHNOLOGIES

Mobile computing devices characteristics – Adaptation – Data dissemination and management – Heterogeneity – Interoperability – Context awareness – Language localization issues – User interface design issues – Difference between UI design for mobile devices and conventional systems – Mobile agents – Mobile device technology overview – Windows CE – Symbian – J2ME – Pocket PC – BREW.

UNIT III SENSOR NETWORKS AND RFID'S

Introduction to sensor networks – Sensor node architecture – Sensor network architecture – Types of sensor networks – Platforms for wireless sensor networks – Applications of wireless sensor networks – Introduction to RFID – Transponder and reader architecture – Types of tags and readers – Frequencies of operation – Application of RFID technologies.

UNIT IV LOCAL AREA AND WIDE AREA WIRELESS TECHNOLOGIES

IEEE 802.11 technologies – Infrared technologies – Bluetooth networks (OBEX protocol) – Personal area networks – Mobility management – Mobile IP – Establishing wide area wireless networks – Concept and structure of "Cell" – Call establishment and maintenance – Channel management – Frequency assignment techniques.

UNIT V PROTOCOLS AND APPLICATIONS

Networking protocols – Packet switched protocols – Routing protocols for sensor networks – Data centric protocols – Hierarchical protocols – Location – Based protocols – Multimedia Messaging Service (MMS) protocols – Wireless Application Protocol (WAP) – Applications of pervasive computing – Retail – Healthcare – Sales force automation – Tracking applications.

REFERENCES

1. Burkhardt, Henn, Hepper and Rintdorff, Schaeck, "Pervasive Computing", Addison Wesley, 2002.

2. F. Adelstein and S.K.S. Gupta, "Fundamentals of Mobile and Pervasive Computing", Tata McGraw Hill, 2005.

3. Ashoke Talukdar and Roopa Yavagal, "Mobile Computing", Tata McGraw Hill, 2005.

UNIT I-PERVASIVE ARCHITECTURE

Local area networks – Wireless LANS – Relationship of wireless, internet and ubiquitous computing – Pervasive computing and ubiquitous computing – Ambient computing – Pervasive web application architecture – Requirements of computational infrastructure – Failure management – Security – Performance – Dependability

Local Area Network

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

A system of LANs connected in this way is called a wide-area network (WAN). Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN.

This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. ARCNET, Token Ring and other technology standards have been used in the past, but Ethernet over twisted pair cabling, and Wi-Fi are the two most common technologies currently used to build LANs.

There are many different types of LANs Ethernets being the most common for PCs. Most Apple Macintosh networks are based on Apple's AppleTalk network system, which is built into Macintosh computers.

The following characteristics differentiate one LAN from another:

- **Topology:** The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.
- **Protocols :** The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.
- **Media :** Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks do without connecting media altogether, communicating instead via radio waves.

.

Larger LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic with VLANs.

Larger LANs also contain a wide variety of network devices such as switches, firewalls, routers, load balancers, and sensors. LANs may have connections with other LANs via leased lines, leased services, or by tunneling across the Internet using virtual private network technologies.

Depending on how the connections are established and secured in a LAN, and the distance involved, a LAN may also be classified as a metropolitan area network (MAN) or a wide area network (WAN).

Cabling

Early LAN cabling had always been based on various grades of coaxial cable. However shielded twisted pair was used in IBM's Token Ring implementation, and in 1984 Star LAN showed the potential of simple unshielded twisted pair by using Cat3-the same simple cable used for telephone systems.

This led to the development of 10Base-T (and its successors) and structured cabling which is still the basis of most commercial LANs today. In addition, fiber-optic cabling is increasingly used in commercial applications. As cabling is not always possible, wireless

Ethernet

Ethernet is the most widely-installed local area network (LAN) technology. Specified in a standard, IEEE 802.3, Ethernet was originally developed by Xerox from an earlier specification called Aloha net (for the Palo Alto Research Center Aloha network) and then developed further by Xerox, DEC, and Intel.

Ethernet was named by Robert Metcalfe, one of its developers, for the passive substance called "luminiferous (light-transmitting) ether" that was once thought to pervade the universe, carrying light throughout. Ethernet was so-named to describe the way that cabling, also a passive medium could similarly carry data everywhere throughout the network

.When first widely deployed in the 1980s, Ethernet supported a maximum theoretical data rate of 10 megabits per second (Mbps).

Later, so-called "Fast Ethernet" standards increased this maximum data rate to 100 Mbps. Today, Gigabit Ethernet technology further extends peak performance up to 1000 Mbps.

Wireless local area network (WLAN)

A wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet.

This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

Wireless LANs have become popular in the home due to ease of installation, and in commercial complexes offering wireless access to their customers; often for free.

Large wireless network projects are being put up in many major cities: New York City, for instance, has begun a pilot program to provide city workers in all five boroughs of the city with wireless Internet access.

WLANs provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling.

A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter.

Network security remains an important issue for Wi- Fi is now the most common technology in residential premises, as the cabling required is minimal and it is well suited to mobile laptops and smart phones.

Stations

All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface controllers (WNICs).

Wireless stations fall into one of two categories: access points, and clients. Access points (APs), normally 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 smart phones, or fixed devices such as desktops 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. 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.

An infrastructure BSS can communicate with other stations not in the same BSS by communicating through access points.

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

Peer-to-Peer / Ad-Hoc

1. **Peer-to-peer**

Peer-to-Peer or ad-hoc wireless LAN

An ad-hoc 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 peer-to-peer (P2P) network allows wireless devices to directly WEP raise the level of security on wireless networks to rival that of traditional wired networks.

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.

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.

Example

A B C

Hidden node problem: Devices A and C are both communicating with B, but are unaware of each other 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.

The 802.11 has two basic modes of operation: Ad hoc mode enables peer-to-peer transmission between mobile units. Infrastructure mode in which mobile units communicate through an access point that serves as a bridge to a wired network infrastructure is the more common wireless LAN application the one being covered. Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also

included shared-key encryption mechanisms: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks.

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. 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.

Roaming

Roaming among Wireless Local Area Networks

There are two definitions for wireless LAN roaming:

Internal Roaming (1): 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) presumes 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.[7]

External Roaming (2): 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.

IEEE 802.11

It is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard **IEEE 802.11-2007** has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand name.

General description

The 802.11 family consists of a series of over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations.

Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signaling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap.[1] Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations.

Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.[2]

Protocols

- **A1 A2** IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.

802.11 protocol	Release	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream (Mbit/s)	Allowable MIMO streams	Modulation	Approximate indoor range (m)	Approximate outdoor range (m)
Jun 1997	2.4	20	1, 2	1	DSSS, FHSS	20	100	
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM QAM	35	120
	3.7			—			5,000	
b	Sep 1999	2.4	20	5.5, 11	1	DSSS	38	140
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM QAM, DSSS	38	140

- [B1 B2] Assumes short guard interval (SGI) enabled, otherwise reduce each data rate by 10%.

802.11a

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage.

However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b.

In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). 802.11a too suffers from interference, but locally there may be fewer signals to interfere with, resulting in less interference and better throughput.

802.11b

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughputs. 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

802.11-2007

In 2003, task group TGma was authorized to "roll up" many of the amendments to the 1999 version of the 802.11 standard. REVma or 802.11ma, as it was called, created a single document that merged 8 amendments (802.11a, b, d,

e, g, h, i, j) with the base standard. Upon approval on March 8, 2007, 802.11REVma was renamed to the then-current base standard **IEEE 802.11-2007**.

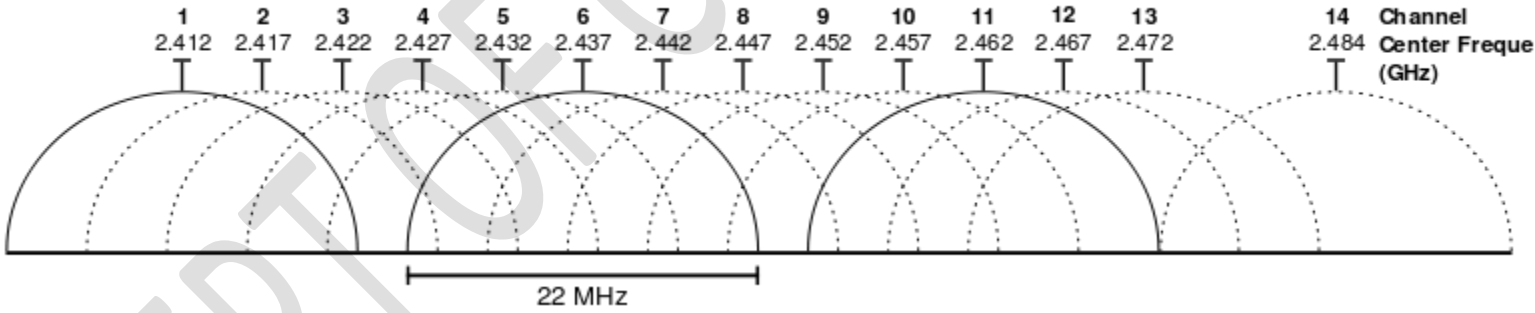
802.11n

802.11n is an amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the lesser used 5 GHz bands. The IEEE has approved the amendment and it was published in October 2009. Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11nproposal.

802.11ac

IEEE 802.11ac is a standard under development which will provide high throughput in the 5 GHz band. This specification will enable multi-station WLAN throughput of at least 1 Gigabit per second and a maximum single link throughput of at least 500 megabit per second, by using wider RF bandwidth, more l streams (up to 8), and high-density modulation (up to 256 QAM).

Channels and international compatibility



.

Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various services.

At one extreme, Japan permits the use of all 14 channels for 802.11b, while other countries such as Spain initially allowed only channels 10 and 11, and France only allowed 10, 11, 12 and 13.

They now allow channels 1 through 13. North America and some Central and South American countries allow only 1 through 11.

Besides specifying the centre frequency of each channel, 802.11 also specify a spectral mask defining the permitted distribution of power across each channel.

The mask requires that the signal be attenuated by at least 30 dB from its peak energy at ±11 MHz from the centre frequency, the sense in which channels are effectively 22 MHz wide.

One consequence is that stations can only use every fourth or fifth channel without overlap, typically 1, 6 and 11 in the Americas, and in theory, 1, 5, 9 and 13 in Europe although 1, 6, and 11 is typical there too.

Another is that channels 1–13 effectively require the band 2.401–2.483 GHz, the actual allocations being, for example, 2.400–2.4835 GHz in the UK, 2.402–2.4735 GHz in the US, etc.

Since the spectral mask only defines power output restrictions up to ±11 MHz from the center frequency to be attenuated by −50 dBr, it is often assumed that the energy of the channel extends no further than these limits.

It is more correct to say that, given the separation between channels 1, 6, and 11, the signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel.

Due to the near-far problem a transmitter can impact a receiver on a "non-overlapping" channel, but only if it is close to the victim receiver (within a meter) or operating above allowed power levels.

A regdomain in IEEE 802.11 is a regulatory region. Different countries define different levels of allowable transmitter power, time that a channel can be occupied, and different available channels.

Domain codes are specified for the United States, Canada, ETSI (Europe), Spain, France, Japan, and China. wifi devices default to regdomain 0, which means least common denominator settings, i.e. the device will not transmit at a power above the allowable power in any nation, nor will it use frequencies that are not permitted in any nation.

The regdomain setting is often made difficult or impossible to change so that the end users do not conflict with local regulatory agencies such as the Federal Communications Commission.

Frames

Current 802.11 standards define "frame" types for use in transmission of data as well as management and control of wireless links. Frames are divided into very specific and standardized sections.

Each frame consists of a MAC header, payload and frame check sequence (FCS). Some frames may not have the payload.

The first two bytes of the MAC header form a frame control field specifying the form and function of the frame. The frame control field is further subdivided into the following sub-fields:

- **Protocol Version:** two bits representing the protocol version. Currently used protocol version is zero. Other values are reserved for future use.
- **Type:** two bits identifying the type of WLAN frame. Control, Data and Management are various frame types defined in IEEE 802.11.
- **Sub Type:** Four bits providing addition discrimination between frames. Type and Sub type together to identify the exact frame.
- **ToDS and FromDS:** Each is one bit in size. They indicate whether a data frame is headed for a distribution system. Control and management frames set these values to zero. All the data frames will have one of these bits set. However communication within an IBSS network always set these bits to zero.
- **More Fragments:** The More Fragments bit is set when a packet is divided into multiple frames for transmission. Every frame except the last frame of a packet will have this bit set.
- **Retry:** Sometimes frames require retransmission, and for this there is a Retry bit which is set to one when a frame is resent. This aids in the elimination of duplicate frames.
- **Power Management:** This bit indicates the power management state of the sender after the completion of a frame exchange. Access points are required to manage the connection and will never set the power saver bit.
- **More Data:** The More Data bit is used to buffer frames received in a distributed system. The access point uses this bit to facilitate stations in power saver mode. It indicates that at least one frame is available and addresses all stations connected.

- **WEP:** The WEP bit is modified after processing a frame. It is toggled to one after a frame has been decrypted or if no encryption is set it will have already been one.
- **Order:** This bit is only set when the "strict ordering" delivery method is employed. Frames and fragments are not always sent in order as it causes a transmission performance penalty.

The next two bytes are reserved for the Duration ID field. This field can take one of three forms: Duration, Contention-Free Period (CFP), and Association ID (AID).

An 802.11 frame can have up to four address fields. Each field can carry a MAC address. Address 1 is the receiver, Address 2 is the transmitter, and Address 3 is used for filtering purposes by the receiver.

- The Sequence Control field is a two-byte section used for identifying message order as well as eliminating duplicate frames. The first 4 bits are used for the fragmentation number and the last 12 bits are the sequence number.
- An optional two-byte Quality of Service control field which was added with 802.11e.
- The Frame Body field is variable in size, from 0 to 2304 bytes plus any overhead from security encapsulation and contains information from higher layers.
- The Frame Check Sequence (FCS) is the last four bytes in the standard 802.11 frame. Often referred to as the Cyclic Redundancy Check (CRC), it allows for integrity check of retrieved frames. As frames are about to be sent the FCS is calculated and appended. When a station receives a frame it can calculate the FCS of the frame and compare it to the one received. If they match, it is assumed that the frame was not distorted during transmission.

• Association request frame: sent from a station it enables the access point to allocate resources and synchronize. The frame carries information about the WNIC including supported data rates and the SSID of the network the station wishes to associate with. If the request is accepted, the access point reserves memory and establishes an association ID for the WNIC.

- Association response frame: sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such an association ID and supported data rates.

- Beacon frame: Sent periodically from an access point to announce its presence and provide the SSID, and other parameters for WNICs within range.
- Deauthentication frame: Sent from a station wishing to terminate connection from another station.
- Disassociation frame: Sent from a station wishing to terminate connection. It's an elegant way to allow the access point to relinquish memory allocation and remove the WNIC from the association table.
- Probe request frame: Sent from a station when it requires information from another station.
- Probe response frame: Sent from an access point containing capability information, supported data rates, etc., after receiving a probe request frame.

3Ubiquitous computing (ubicomp)

Ubiquitous computing (ubicomp) is a post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities.

In the course of ordinary activities, someone "using" ubiquitous computing engages many computational devices and systems simultaneously, and may not necessarily even be aware that they are doing so.

This model is usually considered an advancement from the desktop paradigm. More formally Ubiquitous computing is defined as "machines that fit the human environment instead of forcing humans to enter theirs."

This paradigm is also described as **pervasive computing**, ambient intelligence.,[2] where each term emphasizes slightly different aspects.

When primarily concerning the objects involved, it is also **physical computing**, the Internet of Things, haptic computing,[3] and things that think. Rather than propose a single definition for ubiquitous computing and for these related terms, taxonomy of properties for ubiquitous computing has been proposed, from which different kinds or flavors of ubiquitous systems and applications can be described.

Ubiquitous computing presents challenges across computer science: in systems design and engineering, in systems modeling, and in user interface design.

Contemporary human-computer interaction models, whether command-line, menu-driven, or GUI-based, are inappropriate and inadequate to the ubiquitous case. This suggests that the "natural" interaction paradigm

appropriate to a fully robust ubiquitous computing has yet to emerge - although there is also recognition in the field that in many ways we are already living in an ubicomp world.

Contemporary devices that lend some support to this latter idea include mobile phones, digital audio players, radio-frequency identification tags, GPS, and interactive whiteboards

Mark Weiser proposed three basic forms for ubiquitous system devices, see also Smart device: tabs, pads and boards.

- Tabs: wearable centimetre sized devices
- Pads: hand-held decimetre-sized devices
- Boards: metre sized interactive display devices.

These three forms proposed by Weiser are characterized by being macro-sized, having a planar form and on incorporating visual output displays.

If we relax each of these three characteristics we can expand this range into a much more diverse and potentially more useful range of Ubiquitous Computing devices. Hence, three additional forms for ubiquitous systems have been proposed:

- **Dust**: miniaturized devices can be without visual output displays, e.g., Micro Electro-Mechanical Systems (MEMS), ranging from nanometers through micrometers to millimetres. See also Smart dust.
- **Skin**: fabrics based upon light emitting and conductive polymers, organic computer devices, can be formed into more flexible non-planar display surfaces and products such as clothes and curtains, see OLED display. MEMS device can also be painted onto various surfaces so that a variety of physical world structures can act as networked surfaces of MEMS.
- **Clay**: ensembles of MEMS can be formed into arbitrary three dimensional shapes as artefacts resembling many different kinds of physical object (see also Tangible interface).
- **Reassociation request frame**: A WNIC sends a reassociation request when it drops from range of the currently associated access point and finds another access point with a stronger signal. The new access point coordinates the forwarding of any information that may still be contained in the buffer of the previous access point.

- **Reassociation response frame**: Sent from an access point containing the acceptance or rejection to a WNIC reassociation request frame. The frame includes information required for association such as the association ID and supported data rates.

Control frames facilitate in the exchange of data frames between stations. Some common 802.11 control frames include:

- **Acknowledgement (ACK) frame**: After receiving a data frame, the receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK frame within a predetermined period of time, the sending station will resend the frame.
- **Request to Send (RTS) frame**: The RTS and CTS frames provide an optional collision reduction scheme for access point with hidden stations. A station sends a RTS frame to as the first step in a two-way handshake required before sending data frames.

Ubiquitous, Pervasive and Ambient Computing – Clarification of Terms

Pervasive Computing was pushed in the mid 1990s, more by industry and in particular by IBM. Pervasive computing seems from its origin more focused on technologies and solutions than on a particular vision.

The two major conferences related to this topic: pervasive and percom are more systems and network focused however always keeping some attention to the user experience perspective.

The term ambient intelligence was introduced by the European funding agencies in the Framework 5 vision. Around the same time as the Philips Home-lab that drives the term, too..

Ambient intelligence

In computing, ambient intelligence (AmI) refers to electronic environments that are sensitive and responsive to the presence of people. Ambient intelligence is a vision on the future of consumer electronics, telecommunications and computing that was originally developed in the late 1990s for the time frame 2010–2020. In an ambient intelligence world, devices work in concert to support people in carrying out their everyday life activities, tasks and rituals in easy, natural way using information and intelligence that is hidden in the network connecting these devices (see Internet of

Things). As these devices grow smaller, more connected and more integrated into our environment, the technology disappears into our surroundings until only the user interface remains perceivable by users.

The ambient intelligence paradigm builds upon pervasive computing, ubiquitous computing, profiling practices, context awareness, and human-centric computer interaction design and is characterized by systems and technologies that are

- Embedded: many networked devices are integrated into the environment
- Context aware: these devices can recognize you and your situational context
- Personalized: they can be tailored to your needs

Adaptive: they can change in response to you

- Anticipatory: they can anticipate your desires without conscious mediation.

Ambient intelligence is closely related to the long term vision of an intelligent service system in which technologies are able to automate a platform embedding the required devices for powering context aware, personalized, adaptive and anticipatory services. A typical context of ambient intelligence environment is a Home environment.

The use of the term remained wondrously but steadily low in the first years of the new millennium. Ambient intelligence was used for instance to describe technology that disappears into its surroundings as well as a bridge between the real and digital world.

"Ambient Intelligence" (AmI) is growing fast as a multidisciplinary approach which can allow many areas of research to have a significant beneficial influence into our society.

The basic idea behind AmI is that by enriching an environment with technology (mainly sensors and devices interconnected through a network), a system can be built to take decisions to benefit the users of that environment based on real-time information gathered and historical data accumulated.

Smart Homes

An example of an environment enriched with AmI is a "Smart Home". By Smart Home here we understand a house equipped to bring advanced services to its users.

Naturally, how smart a house should be to qualify as a Smart Home is, so far, a subjective matter. For example, a room can have a sensor to decide when its occupant is in or out and on that basis keep lights on or off.
However, if sensors only rely on movement and no sensor in, say, the door can detect when the person left, then a person reading and keeping the body in a resting position can confuse the system which will leave the room dark.

The system will be confusing absence of movement with absence of the person, that inference will certainly not be considered as particularly "bright", despite the lights. Technology available today is rich.
Several artifacts and items in a house can be enriched with sensors to gather information about their use and in some cases even to act independently without human intervention. Some examples of such devices are electro domestics (e.g., cooker and fridge), household items (e.g., taps, bed and sofa) and temperature handling devices (e.g., air conditioning and radiators). Expected benefits of this technology can be: (a)

Other Environments and Applications for AmI

Other applications are also feasible and relevant and the use of sensors and smart devices can be found in:

- Health-related applications. Hospitals can increase the efficiency of their services by monitoring patients' health and progress by performing automatic analysis of activities in their rooms. They can also increase safety by, for example, only allowing authorized personnel and patients to have access to specific areas and devices.

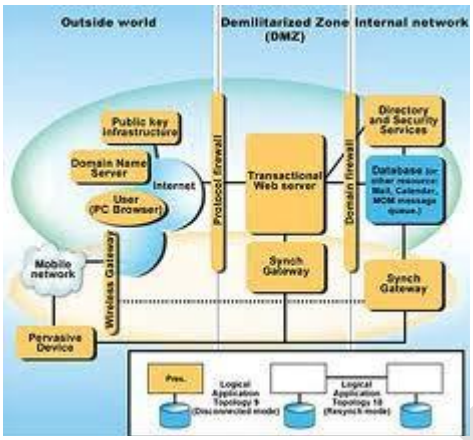
- Public transportation sector. Public transport can benefit from extra technology including satellite services, GPS-based spatial location, vehicle identification, image processing and other technologies to make transport more fluent and hence more efficient and safe.

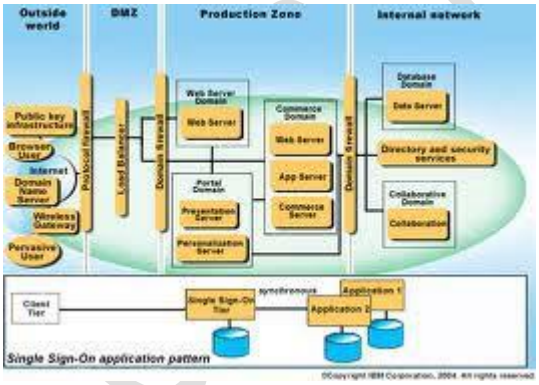
- Education services. Education-related institutions may use technology to track students progression on their tasks, frequency of attendance to specific places and health related issues like advising on their diet regarding their habits and the class of intakes they opted for.

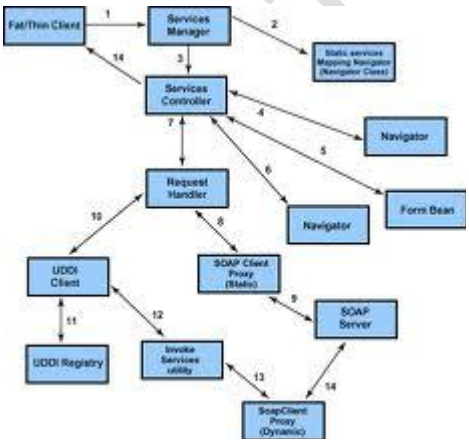
- Emergency services. Safety-related services like fire brigades can improve the reaction to a hazard by locating the place more efficiently and also by preparing the way to reach the place in connection with street services.

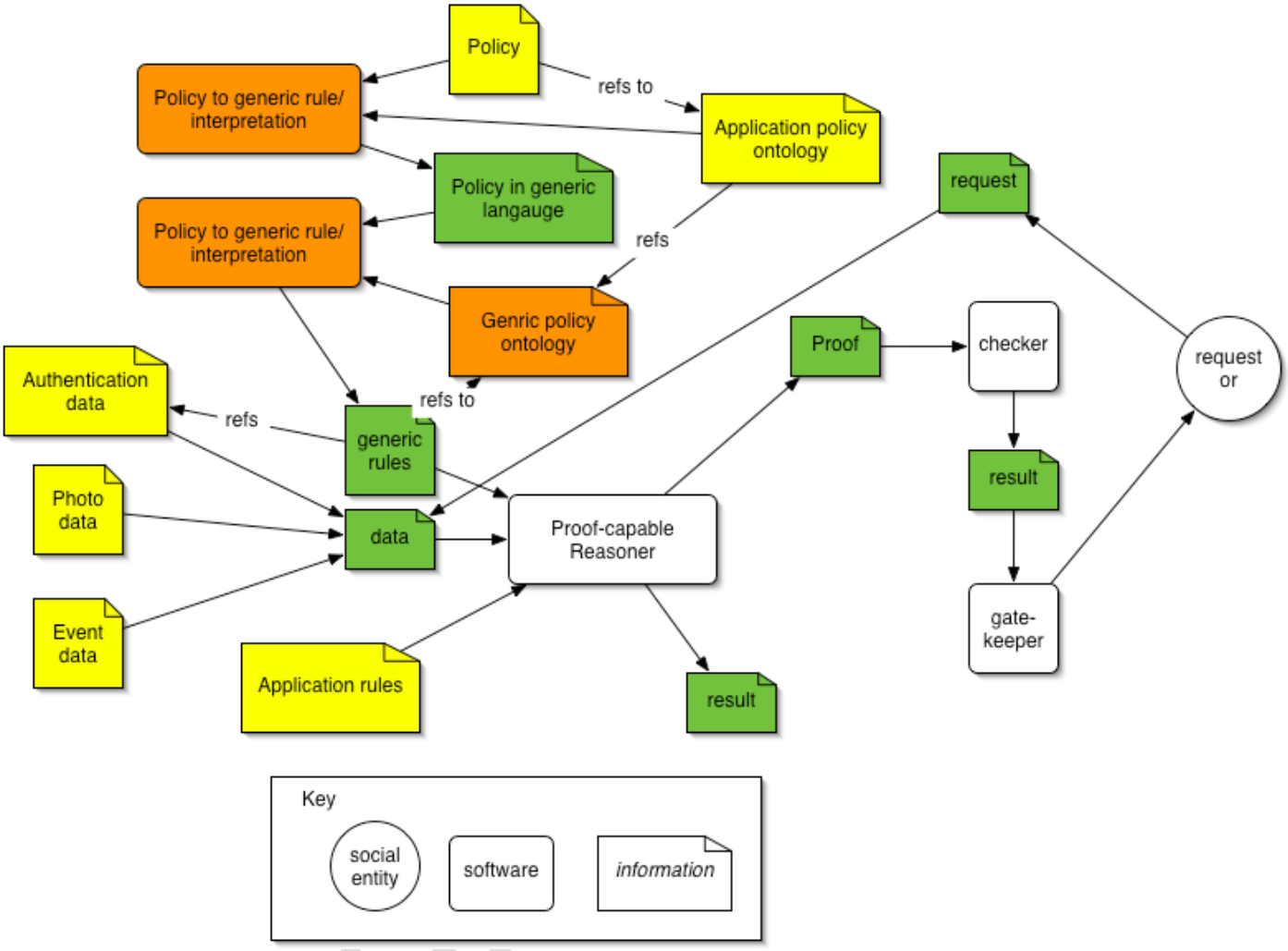
The prison service can also quickly locate a place where a hazard is occurring or is likely to occur and prepare better access to it for security personnel.

• Production-oriented places. Production-centered places like factories can self-organize according to the production/demand ratio of the goods produced. This will demand careful correlation between the collection of data through sensors within the different sections of the production line and the pool of demands via a diagnostic system which can advice the people in charge of the system at a decision-making level.









A web application is an application that is accessed over a network such as the Internet or an intranet . The term may also mean a computer software application that is coded in a browser-supported language (such as JavaScript, combined with a browser-rendered markup language like HTML) and reliant on a common web browser to render the application executable.

Web applications are popular due to the ubiquity of web browsers, and the convenience of using a web browser as a client, sometimes called a thin client.

The ability to update and maintain web applications without distributing and installing software on potentially thousands of client computers is a key reason for their popularity, as is the inherent support for cross-platform compatibility. Common web applications include webmail, online retail sales, online auctions, wikis and many other functions.

Structure

Applications are usually broken into logical chunks called "tiers", where every tier is assigned a role. Traditional applications consist only of 1 tier, which resides on the client machine, but web applications lend themselves to an n-tiered approach by nature.

Though many variations are possible, the most common structure is the three-tiered application. In its most common form, the three tiers are called presentation, application and storage, in this order.

A web browser is the first tier (presentation), an engine using some dynamic Web content technology (such as ASP, ASP.NET, CGI, ColdFusion, JSP/Java, PHP, Perl, Python, Ruby on Rails or Struts2) is the middle tier (application logic), and a database is the third tier (storage).

The web browser sends requests to the middle tier, which services them by making queries and updates against the database and generates a user interface.

APPLICATION SCENARIOS

Supermarket Scenario. The consumer enters the supermarket and selects a “smart” shopping cart (a smart shopping cart is equipped with radio frequency identification (RFID) readers and an on board personal digital assistant (PDA). She identifies to the system using her RFID enabled loyalty card (her user ID is read into the PDA and transmitted to the authentication server) on the cart and gains access by entering her personal identification number (PIN).

The system logs her in, responds with a welcome message and then proceeds to present a “suggested” shopping list, based on monitored home inventory and actual consumption data

The consumer walks in the supermarket aisles and picks up products from the shelves. For example, she may decide to buy a shampoo, which she picks up and places inside her shopping cart.

By doing so, the RFID readers on the cart identify the entry of the shampoo bottle and trigger the following sequence: the ID is sent to the back end systems, the systems retrieve information about the specific product and update the display of the shopping list and of the total cost of the shopping cart content.

Next, the consumer decides to buy a hair conditioner where the retailer has placed a discount promotion for customers with her profile. When the consumer places the product in the cart, the system displays the promotion on the PDA screen as well as instructions on the shortest path to the aisle and self where the product is held.

Later, the consumer decides to remove one can of orange juice from her cart and replace it on the supermarket shelves. The system updates the shopping list with the new total amount and the new contents of the cart.

When the items on the shopping list are exhausted, the consumer proceeds to the check out.

Home Scenario. The consumer returns home and places her shopping in her RFID enabled storage (fridge, cupboard etc). New product information is recorded by her home server and consolidated to the home inventory data. The home maintains data on inventory levels as well as consumption. Periodically, the consumer gives permission to her home server to upload her new shopping list to the system.

On-the-move Scenario. While on her way to work, the consumer uses her mobile phone to check which products she needs to replenish before the weekend. After logging in, the list.

The consumer decides to add new items to her shopping list for the dinner party she gives on Saturday night. The consumer is happy with her new shopping list.

The system displays the total cost of her shopping list at her usual supermarket. The consumer is unhappy with the price and she decides to look for a better price, thus initiating a reverse auction.

The system forwards her list to participating retailers and prompts the consumer to define the duration of the auction, which she does.

The system sends a confirmation message that the process has been initiated. A short while later the consumer receives offers by different retailers and selects the best.

Fault Tolerance

Faults can lead to incorrect context sensing, security and privacy breaches and misuse of resources. Therefore, fault containment is a very important aspect of deploying a pervasive system into the physical world.

Classification of Failures

A typical pervasive system consists of commercial off-the-shelf (COTS) software and devices whose reliability is not guaranteed. COTS software are sold as "black boxes" and may not be subject to rigid development, verification or testing processes. Interoperability issues further reduce the reliability of a pervasive system.

Mobile devices such as handhelds and laptops, with limited battery power, cannot be regarded as totally reliable. Connectivity failures due to devices going out of range or other errors in networks add to faults in a pervasive system.

1**. Device Failures**

A pervasive system consists of different kinds of devices such as desktops, laptops, handhelds, sensors, actuators, displays, speakers, scanners, cameras and projectors. Each device has its own set of faults that can potentially contribute to the failure of the pervasive system.

Mobile devices, such as laptops and handhelds, have physical constraints such as finite battery power and limited signal strength. So if the battery goes down or if the signal strength is too low they get disconnected from the pervasive system and are regarded as having failed.

A more acute problem with devices is when they are alive but operates incorrectly. This is common in faulty sensors and is called a Byzantine failure.

2. **Application Failures**

Designing reliable software is an expensive process and the cost of debugging, testing and verifying can easily range from 50 to 75 percent of the total development cost. Even in well-tested software systems, bugs of varying severity are found. Pervasive computing includes commercial off-the-shelf applications that may not be well tested.

3. Network Failures

Pervasive systems consist of wired and wireless devices. Therefore, a reliable pervasive system should account for network failures caused by low signal strength, devices going out of range and unavailability of communication

channels due to heavy traffic. Network failures lead to unreachable devices that may be wrongly perceived as device failures. Automatic detection of the failure type is an important issue in pervasive computing.

4. Service Failures

As mentioned above, a pervasive system is supported by various services that enable different functionalities. Some of these services are essential while others add features to a pervasive system. Essential services include naming, event and discovery services. Some pervasive systems support other services such as a trading service that enables device discovery, context services that enable context-aware computing and file system services for ubiquitous data access.

Implications of Failures

Digital devices co-exist with physical devices to aid in accomplishing everyday tasks. Therefore, faults in pervasive systems can be bothersome and result in user annoyance. Failure to correctly identify the person can result in a different configuration and can be a source of annoyance to the user.

Security Vulnerabilities

The ubiquity of deployment of pervasive systems necessitates robust security mechanisms for access control and authentication. Faults can lead to security breaches and consequent compromise of trust. A failed intrusion detection system may not detect an intruder while failure in an authentication system may let users misuse resources and data.

Challenges Facing Fault Tolerance

The fault model only considers application failures caused by transient errors such as device failures, network faults and failures due to faulty usage. Applications periodically save their states onto a checkpoint storage. The reliability of the storage can be improved by traditional techniques such as RAID and so we do not address its failures.

The fault manager obtains information about the current context from the context infrastructure and it gets device and application properties from the Space Repository. It uses this information to infer a contextually appropriate surrogate device on which the application can be restarted.

The failed application is then restarted on the surrogate device using the saved state from the checkpoint storage. This is called rollback recovery and reduces loss of state on failure. The fault management system uses a Prolog based

reasoning mechanism to determine the most appropriate surrogate device. It considers parameters such as availability of the device, user preferences and application capability while reasoning.

UNIT II MOBILE DEVICE TECHNOLOGIES

UNIT II MOBILE DEVICE TECHNOLOGIES

Mobile computing devices characteristics – Adaptation – Data dissemination and management – Heterogeneity – Interoperability – Context awareness – Language localization issues – User interface design issues – Difference between UI design for mobile devices and conventional systems – Mobile agents – Mobile device technology overview – Windows CE – Symbian – J2ME – Pocket PC – BREW.

Mobile computing devices characteristics

- The term "Mobile computing" is used to describe the use of computing devices which usually interact in some fashion with a central information system while away from the normal, fixed workplace.

- Mobile computing technology enables the mobile worker to: (a) create; (b) access; (c) process; (d) store; and (e) communicate information without being constrained to a single location.

Portability

- Mobile devices are defined by their ability to be moved frequently. Any mobile device should function and operate consistently while on the move, regardless of proximity to a power source or physical Internet connection.
- To aid in portability, mobile devices typically contain rechargeable batteries that allow several hours or more of operation without access to an external charger or power source.

Small Size

- Mobile devices are also known as handhelds, palmtops and smart phones due to their roughly phone-like dimensions. A typical mobile device will fit in the average adult's hand or pocket.

- Some mobile devices may fold or slide from a compact, portable mode to a slightly larger size, revealing built-in keyboards or larger screens.
- Mobile devices make use of touch screens and small keypads to receive input, maintaining their small size and independence from external interface devices.
- The standard form of a mobile device allows the user to operate it with one hand, holding the device in the palm or fingers while executing its functions with the thumb.
- Net books and small tablet computers are sometimes mistaken for true mobile devices, based on their similarity in form and function, but if the device's size prohibits one-handed operation or hinders portability, then it cannot be considered a true mobile device.

Wireless Communication

- Mobile devices are typically capable of communication with other similar devices, with stationary computers and systems, with networks and portable phones.
- Base mobile devices are capable of accessing the Internet through Bluetooth or Wi-Fi networks, and many models are equipped to access cell phone and wireless data networks as well.
- Email and texting are standard ways of communicating with mobile devices, although many are also capable of telephony, and some specialized mobile devices, such as RFID and barcode readers, communicate directly with a central device.

Adaptation

- Mobile computing platforms such as mobile phones, PDAs or wearable computers operate in a much more volatile and limited environment than their stationary counterparts.
- Such platforms are inherently resource poor and subject to highly changeable resource availability. Applications for Mobile Computing require adaptation for best performance under such variable conditions, to make best use of available resources without assuming the minimum set.

Distributed Systems

- A distributed system (DS) consists of a collection of autonomous components, connected through a computer network. These components may have different hardware architectures and operating systems (OSs).

- In a distributed system, the components may be shared, and the user perceives the whole system as a single computing facility]. The main challenges introduced by the distribution are related to the following aspects: heterogeneity, openness, scalability, resource sharing, concurrency, security, fault-tolerance, and transparency.

- **Middleware Systems**

- When developing applications for distributed systems, the aspects introduced by the distribution must be addressed. Middleware systems can be distinguished based on the type of computational load they can execute, the ommunication paradigms they support, and the type of context representation they provide to the applications

Data dissemination and management

- Data dissemination on the internet is possible through many different kinds of communications protocols. The internet protocols are the most popular non-proprietary open system protocol suite in the world today. They are used in data dissemination through various communication infrastructures across any set of interconnected networks.

- Despite the name internet protocol, they are also well suited for local area networks (LAN) and wide area network (WAN) communication.

- Using the internet, there are several ways data can be disseminated. The World Wide Web is an interlinked system where documents, images and other multimedia content can be accessed via the internet using web browsers.
- It uses a markup language called hyper text markup language (HMTL) to format disparate data into the web browser.
- The Email (electronic mail) is also one of the most widely used systems for data dissemination using the internet and electronic medium to store and forward messages.
- The email is based on the Simple Mail Transfer Protocol (SMTP) and can also be used by companies within an intranet system so that staff could communicate with other.

- Data dissemination is a very substantial aspect of business operation. Most of today's businesses are data driven. It is a common scenario where business organizations invest millions for data warehouses including hardware, software and manpower costs, to make data dissemination fast, accurate and timely..

- Data dissemination in asymmetrical communication environment, where the downlink communication capacity is much greater than the uplink communication capacity, is best suited for mobile environment

- There are three kinds of broadcast models, namely push-based broadcast, On-demand (or pull-based) broadcast, and hybrid broadcast.

Push based data scheduling

- In push based data broadcast, the server broadcasts data proactively to all clients according to the broadcast program generated by the data scheduling algorithm. The broadcast program essentially determines the order

and frequencies that the data items are broadcast in. The scheduling algorithm may make use of precompiled access profiles in determining the broadcast program.

On-demand data scheduling

- A wireless on demand broadcast system supports both broadcast and on demand services through a broadcast channel and a low bandwidth uplink channel. The uplink channel can be a wired or a wireless link. When a client needs a data item, it sends to the server an on demand request for the item through the uplink. Client requests are queued up (if necessary) at the server upon arrival.
- The server repeatedly chooses an item from among the outstanding requests, broadcasts it over the broadcast channel, and removes the associated request(s) from the queue.

Hybrid data scheduling

- Push-based data broadcast cannot adapt well to a large database and a dynamic environment. On-demand data broadcast can overcome these problems. However, it has two main disadvantages:

- more uplink messages are issued by mobile clients, thereby adding demand on the scarce uplink bandwidth and consuming more battery power on mobile clients
- ii) if the uplink channel is congested, the access latency will become extremely high. A promising approach, called hybrid broadcast, is to combine push-based and on-demand techniques so that they can complement each other.

Heterogeneity in Mobile Devices

- The presence of heterogeneity implies that some devices are more powerful than others, and some can be servers while others can only be clients. In addition, relaying packets for others can result in a device expelling

its own energy. Hence, a mobile node should examine its own "well-being" before committing to forwarding packets on the behalf of others.

- Heterogeneity arises in a wide range of scenarios in mobile opportunistic networks and is one of key factors that govern the performance of packet forwarding algorithms.
- While the heterogeneity has been empirically investigated and exploited in the design of new forwarding algorithms, it has been typically ignored or marginalized when it comes to rigorous performance analysis of such algorithms

Interoperability

- The ability of a network to operate with other networks, such as two systems based on different protocols or technologies. Each data-centric mobile middleware has a unique abstraction of the data.
- They vary in data format, mode of operation etc. As each of these middleware has some advantage over others, it is important to establish interoperability among these.
- There might be application-level interconnection among these components. But that is disadvantageous.

Context awareness

- Context awareness is defined complementary to location awareness. Whereas location may serve as a determinant for resident processes, context may be applied more flexibly with mobile computing with any moving entities, especially with bearers of smart communicators.

Qualities of context

- Context defines some rules of inter-relationship of features in processing any entities as a binding clause.
- Some classical understanding of context in business processes is derived from the definition of AAA applications[4] with the following three categories:
    - Authentication, which means i.e. confirmation of stated identity

- Authorizations, which means i.e. allowance to accrual or access to location, function, data
- Accounting, which means i.e. the relation to order context and to accounts for applied labour, granted license, and delivered goods.

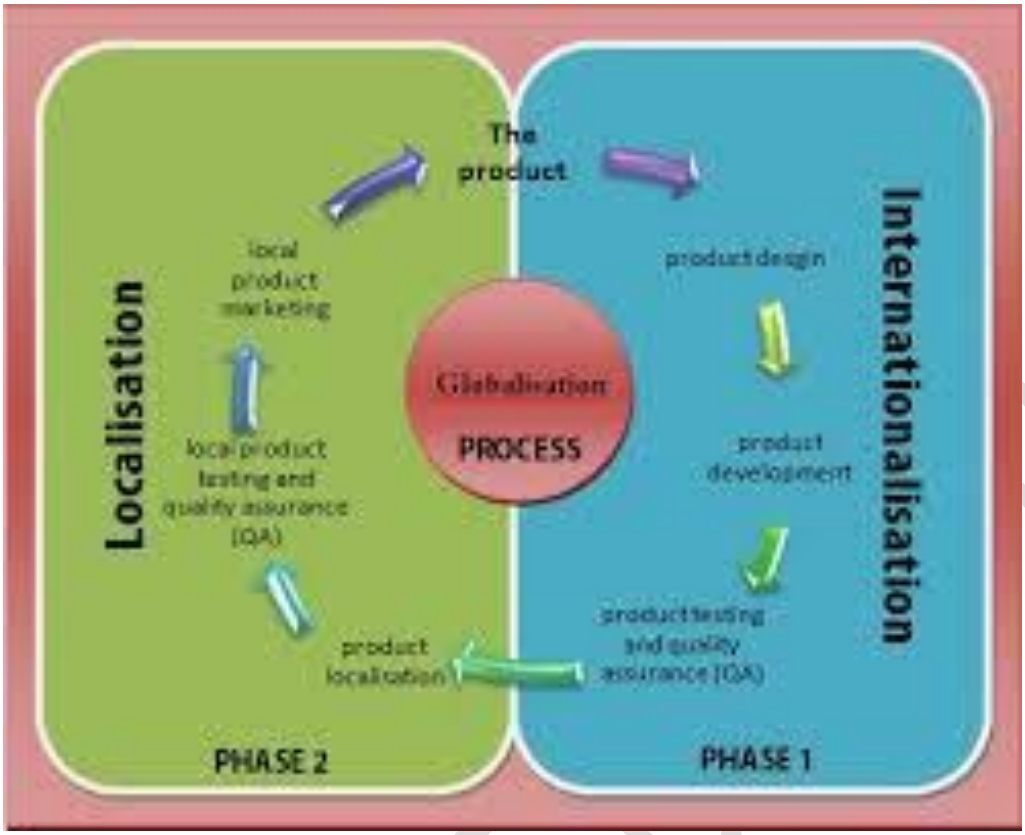
❖ Context aware systems are concerned with the acquisition of context (e.g. using sensors to perceive a situation), the abstraction and understanding of context (e.g. matching a perceived sensory stimulus to a context), and application behaviour based on the recognized context (e.g. triggering actions based on context).[10] As the user's activity and location are crucial for many applications, context awareness has been focused more deeply in the research fields of location awareness and activity recognition.

Language localization issues

❖ **Language localisation** (from Latin *locus* (place) and the English term *locale*, "a place where something happens or is set")[1] is the second phase of a larger process of product translation and cultural adaptation (for specific countries, regions, or groups) to account for differences in distinct markets, a process known as internationalization and localisation.

❖ The localisation process is most generally related to the cultural adaptation and translation of software, video games, and websites, and less frequently to any written translation Localisation can be done for regions or countries where people speak different languages, or where the same language is spoken

❖ As the former Localisation Industry Standards Association explained, globalization "can best be thought of as a cycle rather than a single process".[2] To globalize is to plan the design and development methods for a product in advance, keeping in mind a multicultural audience, in order to avoid increased costs and quality problems, save time, and smooth the localizing effort for each region or country. Localisation is an integral part of the overall process called **globalizations**.



- The first phase, **internationalization**, encompasses the planning and preparation stages for a product that is built by design to support global markets. This process removes all cultural assumptions and any country- or language-specific content is stored so that it can be easily adapted. If this content is not separated during this phase, it must be fixed during localisation, adding time and expense to the project. In extreme cases, products that were not internationalized may not be localisable.
- The second phase, **localisation**, refers to the actual adaptation of the product for a specific market. The localisation phase involves, among other things, the four issues LISA describes *as* linguistic, physical, business and cultural and technical issues.
- At the end of each phase, testing, including quality assurance, is performed to ensure that product works properly and meets the client's quality expectations.

User interface design issues

The single most important concept to master when designing mobile device interfaces is “context”. The context in which an application is used and the context of how information is input are both key issues;

Context of Use

- Mobile devices are excellent at connecting users to information; and while consumption of information is likely the largest segment of mobile device usage, interacting with a mobile device to perform important tasks is a usage segment that deserves significant attention.
- This is because generative work conducted on mobile devices tends to be tactical in nature and demands a sense of immediacy.
- Users have a very specific need and desire to accomplish their goal in the easiest and fastest way possible. This fact alone helps explain why mobile interfaces are designed the way they are:
  - Feature sets are optimized to streamline common use cases
  - Use typography to show hierarchy and importance
  - Features are progressively displayed
  - Large buttons are used to make interactions actionable

Difference between UI design for mobile devices and conventional systems

- Expert systems are computerized tools designed to enhance the quality and availability of knowledge required by decision makers in a wide range of industries. They augment conventional programs such as databases, word processors, and spreadsheet analysis. Expert systems differ from conventional applications software in the following ways.
- The expert system shell or interpreter. The existence of a "knowledge base," or system of related concepts that enable the computer to approximate human judgment. The sophistication of the user interface.

- While any conventional programming language can be used to build a knowledge base, the expert system shell simplifies the process of creating a knowledge base.
- It is the shell that actually processes the information entered by a user; relates it to the concepts contained in the knowledge base; and provides an assessment or solution for a particular problem.
- The main purpose of the knowledge base is to provide the guts of the expert system--the connections between ideas, concepts, and statistical probabilities that allow the reasoning part of the system to perform an accurate evaluation of a potential problem.
- Knowledge bases are traditionally described as large systems of "if then" statements, but this description is misleading because knowledge bases may not contain definitive rules at all, but may contain only associative relationships among different concepts, statistical information about the probability of certain solutions, or simply large databases of facts that can be compared to one another based on simple conventions intrinsic to the expert system.

Mobile agent

- **Mobile agent** is a composition of computer software and data which is able to migrate (move) from one computer to another autonomously and continue its execution on the destination computer.
- A Mobile Agent, namely, is a type of software agent, with the feature of autonomy, social ability, learning, and most importantly, mobility.
- A mobile agent is a process that can transport its state from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. Mobile agents decide when and where to move.

Advantages

Some **advantages** which mobile agents have over conventional agents:

- Computation bundles - converts computational client/server round trips to relocatable data bundles, reducing network load.
- Parallel processing -asynchronous execution on multiple heterogeneous network hosts

- Dynamic adaptation - actions are dependent on the state of the host environment
- Tolerant to network faults - able to operate without an active connection between client and server
- Flexible maintenance - to change an agent's actions, only the source (rather than the computation hosts) must be updated

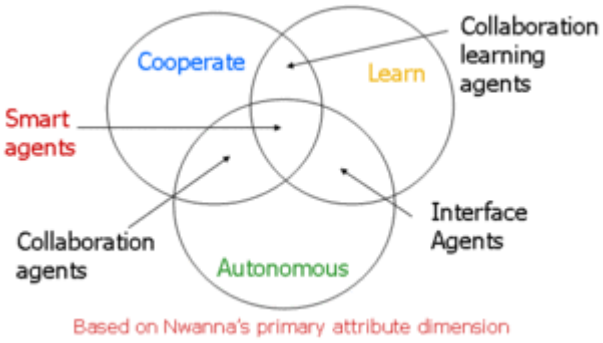
Software agent

Software agent is a software program that acts for a user or other program in a relationship of agency, which derives from the Latin agree (to do): an agreement to act on one's behalf. Such "action on behalf of" implies the authority to decide which, if any, action is appropriate.

- **Intelligent agents** (in particular exhibiting some aspect of Artificial Intelligence, such as learning and reasoning)
- **Autonomous agents** (capable of modifying the way in which they achieve their objectives),
- **Distributed agents** (being executed on physically distinct computers)
- **Multi-agent systems** (distributed agents that do not have the capabilities to achieve an objective alone and thus must communicate)
- **Mobile agents** (agents that can relocate their execution onto different processors).

The basic attributes of a software agent are that

- Agents are not strictly invoked for a task, but activate themselves,
- Agents may reside in wait status on a host, perceiving context,
- Agents may get to run status on a host upon starting conditions,
- Agents do not require interaction of user,
- Agents do may invoke other tasks including communication.



Mobile code

- **Mobile code** is software transferred between systems, e.g. transferred across a network or via a USB flash drive, and executed on a local system without explicit installation or execution by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded within Microsoft Office documents.

Remote evaluation

Remote evaluation is a general term for any technology that involves the transmission of executable software programs from a client computer to a server computer for subsequent execution at the server.

- After the program has terminated, the results of its execution are sent back to the client.
- Remote evaluation belongs to the family of mobile code and web service technologies.
- An example for remote evaluation is grid computing: An executable task may be sent to a specific computer in the grid. After the execution has terminated, the result is sent back to the client.
- The client in turn may have to reassemble the different results of multiple concurrently calculated subtasks into one single result.

Windows CE

- Microsoft Windows CE (now officially known as Windows Embedded Compact and previously also known as Windows Embedded CE, and sometimes abbreviated WinCE) is an operating system developed by Microsoft for embedded systems.
- Windows CE is a distinct operating system and kernel, rather than a trimmed-down version of desktop Windows. It is not to be confused with Windows Embedded Standard which is an NT-based componentized version of desktop Microsoft Windows.
- Microsoft licenses Windows CE to OEMs and device makers. The OEMs and device makers can modify and create their own user interfaces and experiences, with Windows CE providing the technical foundation to do so.

Features

- Windows CE is optimized for devices that have minimal storage; a Windows CE kernel may run in under a megabyte of memory. Devices are often configured without disk storage, and may be configured as a "closed" system that does not allow for end-user extension (for instance, it can be burned into ROM).
- Windows CE conforms to the definition of a real-time operating system, with deterministic interrupt latency. From Version 3 and onward, the system supports 256 priority levels[7] and uses priority inheritance for dealing with priority inversion.
- The fundamental unit of execution is the thread. This helps to simplify the interface and improve execution time.

Symbian

- **Symbian** is a mobile operating system (OS) and computing platform designed for smart phones and currently maintained by Accenture.
- Symbian platform is the successor to Symbian OS and Nokia Series 60; unlike Symbian OS, which needed an additional user interface system, Symbian includes a user interface component based on S60 5th Edition.
- The latest version, Symbian^3, was officially released in Q4 2010, first used in the Nokia N8. In May 2011 an update, Symbian Anna, was officially announced, followed by Nokia Belle (previously Symbian Belle) in August 2011
- .Symbian OS was originally developed by Symbian Ltd.[10] Psion's EPOC and runs exclusively on ARM processors, although an unreleased x86 port existed.

J2ME

- Java Platform, Micro Edition (Java ME) provides a robust, flexible environment for applications running on mobile and embedded devices: mobile phones, set-top boxes, Blu-ray Disc players, digital media devices, M2M modules, printers and more.

- Java ME technology was originally created in order to deal with the constraints associated with building applications for small devices.
- For this purpose Oracle defined the basics for Java ME technology to fit such a limited environment and make it possible to create Java applications running on small devices with limited memory, display and power capacity.
- Java 2 Micro Edition (J2ME) combines a resource-constrained JVM and a set of Java APIs for developing applications for mobile devices. This article is the first in a series.

- J2ME combines a resource constrained JVM and a set of Java APIs for developing applications for mobile devices.
- J2ME can be divided into three parts, as shown in Figure 1: a configuration, a profile, and optional packages.
- A configuration contains the JVM (not the traditional JVM, but the cut-down version) and some class libraries; a profile builds on top of these base class libraries by providing a useful set of APIs; and optional packages, are well, an optional set of APIs that you may or may not use when creating your applications.

Optional packages are traditionally not packaged by the device manufacturers, and you have to package and distribute them with your application.

The configuration and profile are supplied by the device manufacturers and they embedded them in the devices.

Figure

- The most popular profile and configuration that Sun provides are the Mobile Information Device Profile (MIDP) and Connected Limited Device Configuration (CLDC), respectively.
- As the name suggests, CLDC is for devices with limited configurations; for example, devices that have only 128 to 512KB of memory available for Java applications. Consequently, the JVM that it provides is very limited and supports only a small number of traditional Java classes. (This limited JVM is actually called the KVM.)
- Its counterpart, the Connected Device Configuration (CDC) is for devices with at least 2MB of memory available and supports a more feature-rich JVM (but still not a standard JVM).
- The MID profile complements the CLDC configuration very well because it minimizes both the memory and power required for limited devices. It provides the basic API that is used for creating application for these devices.
- The latest versions of MIDP and CLDC are 2.0 and 1.1, respectively. Not many devices currently support these versions, but the list is growing rapidly. Sun maintains a list of devices according to version.

Pocket PC

- Pocket PC are used interchangeably, in part due to their common origin. This practice is not entirely accurate. Windows CE is a modular/componentized operating system that serves as the foundation of several classes of devices.
- Some of these modules provide subsets of other components' features (e.g. varying levels of windowing support; DCOM vs COM), others which are separate (Bitmap or TrueType font support), and others which add additional features to another component.
- One can buy a kit (the Platform Builder) which contains all these components and the tools with which to develop a custom platform.
- Applications such as Excel Mobile/Pocket Excel are not part of this kit. The older Handheld PC version of Pocket Word and several other older applications are included as samples.

- Pocket PC and Windows Mobile are Microsoft-defined custom platforms for general PDA use, consisting of a Microsoft-defined set of minimum profiles (Professional Edition, Premium Edition) of software and hardware that is supported.
- The rules for manufacturing a Pocket PC device are stricter than those for producing a custom Windows CE-based platform. The defining characteristics of the Pocket PC are the touch screen as the primary human interface device and its extremely portable size.

BREW

- **Brew** (**Brew MP**, Binary Runtime Environment for Wireless) is an application development platform created by Qualcomm, originally for CDMA mobile phones, featuring third party applications such as mobile games.
- It is offered in some feature phones but not in smart phones. It debuted in September 2001.
- As a software platform that can download and run small programs for playing games, sending messages, and sharing photos, the main advantage of Brew MP is that the application developers can easily port their applications among all Brew MP devices by providing a standardized set of application programming interfaces.
- Software for the Brew MP enabled handsets can be developed in C or C++ using the freely downloadable Brew MP SDK.[1]
- The Brew runtime library is part of the wireless device on-chip firmware or operating system in order to allow programmers to develop applications without needing to code for system interface or understand wireless applications. Brew is described as a pseudo operating system, but not a true mobile operating system.
- Brew is not a virtual machine such as Java ME, but runs native code.

Brew application development

- For testing applications during the development process, the SDK includes a Brew Emulator, or starting with Brew Version 3.1.5 and above, the Brew Simulator.
- The Brew Emulator (currently called Brew Simulator) does not emulate handset's hardware. Instead, the Brew application is compiled to native code and linked with a compatible Brew runtime library. Because of this, applications cannot be tested for platform bugs related to memory alignment and various firmware related glitches without a Brew handset operating in test mode.
- For testing purposes, Brew applications can be transferred using a USB or serial cable to any Brew-compatible handset using Brew AppLoader from Qualcomm.
- A Brew application contains several components which, if not present and valid, cause the application to be automatically deleted on reboot.
- This includes the compiled binary file, a file which describes the application, the features it uses and permissions requested a file that contains string and image resources if required, and a file containing the application's digital signature.
- Brew Applications may be unloaded from a consumer handset to save handset memory space. This is referred to as "Disable/Restore", and is a requirement of the True Brew Test Process.
- Saved files are kept intact using Disable/Restore, and it is possible to re-load the application without paying for it again. In a "Disable" situation, all .bar, .mod, and .sig files are deleted from the handset, while any other files remain in their original place. During the "Restore" operation, the .bar, .mod, and.sig files are downloaded from the carrier's mobile store, and the previously disabled application will have full functionality remaining.
- The Disable/Restore process is only available to consumer users once the handset's memory is completely.

UNIT III SENSOR NETWORKS AND RFID'S

Introduction to sensor networks – Sensor node architecture – Sensor network architecture – Types of sensor networks – Platforms for wireless sensor networks – Applications of wireless sensor networks – Introduction to RFID – Transponder and reader architecture – Types of tags and readers – Frequencies of operation – Application of RFID technologies.

Introduction to sensor networks

- In computer networking there is a great value of wireless networking because it has no difficult installation, no more expenditure and has lot of way to save money and time. In the field of wireless networking there is another form of networking which is called as wireless sensor network.
- A type of wireless networking which is comprised on number of numerous sensors and they are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors.
- This type of networking is called as Wireless sensor networking. Basically wireless sensor networking is used for monitoring the physical conditions such as weather conditions, regularity of temperature, different kinds of vibrations and also deals in the field of technology related to sound.

Definition

- Wireless Sensor Networks (WSNs):
  - Highly distributed networks of small, lightweight wireless nodes,
  - Deployed in large numbers,
  - Monitors the environment or system by measuring physical parameters such as temperature, pressure, humidity.
- Node: sensing + processing + communication

How wireless sensor network works?

- Total working of wireless sensor networking is based on its construction. Sensor network initially consists of small or large nodes called as sensor nodes.

- These nodes are varying in size and totally depend on the size because different sizes of sensor nodes work efficiently in different fields.
- Wireless sensor networking have such sensor nodes which are specially designed in such a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also equipped with an energy source such as battery.
- The entire network worked simultaneously by using different dimensions of sensors and worked on the phenomenon of multi routing algorithm which is also termed as wireless ad hoc networking.

Applications of Wireless Sensor Networking:

- In the present era there are lot of technologies which are used for monitoring are completely based on the wireless sensor networking.
- Some of important applications are environmental monitoring, traffic control application, weather checking, regularity checking of temperature etc.
- Wireless sensor networks can also be used for detecting the presence of vehicles such as motor cycles up to trains.
- These are some important wireless sensor networking based technologies which help us in our daily life.
- Some of there daily life applications are: used in agriculture, water level monitoring, green house monitoring, landfill monitoring etc.

Future of wireless sensor networks

- But wireless sensor networking has a bright future in the field of computer networking because we can solve the monitoring problems at an advanced level in the future with the help of such technology of networking.

Wireless Sensor Network Topologies

- The development of network technologies has prompted sensor folks to consider alternatives that reduce costs and complexity and improve reliability. Early sensor networks used simple twisted shielded–pair (TSP) implementations for each sensor. Later, the industry adopted multidrop buses (e.g., Ethernet).

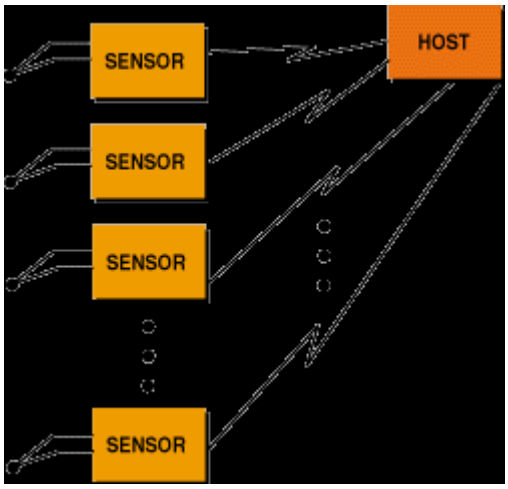
❖ 

Figure 1. In point-to-point network topologies, each sensor node requires a separate twisted shielded–pair wire connection. The cost is high, configuration management is difficult, and nearly all the information processing is done by the host.

Point-to-Point Networks

- ❖ Theoretically, these systems are the most reliable because there is only one single point of failure in the topology—the host itself (see Figure 1).
- ❖ You can improve the system by adding redundant hosts, but wiring two hosts can be a problem. The 4–20 mA standard allows multiple readout circuits if the standard loads are used at each readout.
- ❖ Problems can arise if readout devices load the circuit beyond its capability, but most designers are familiar with the limitations and are sufficiently careful.

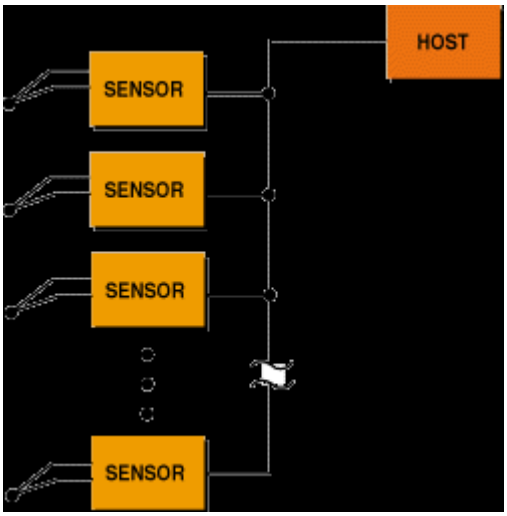


Figure 2. In a multidrop network, each sensor node puts its information onto a common medium. This requires careful attention to protocols in hardware and software. The single-wire connection represents a potential single-point failure. But some vendors supply redundant connections to mitigate this potential problem.

- Multidrop buses began to appear in the late 70s and early 80s. The emergence of intelligent sensors and microcomputers capable of operating in industrial environments irrevocably changed the sensor network landscape.
- Multidrop networks (buses) reduced the number of wires required to connect field devices to the host, but they also introduced another single point of failure—the cable.
- Several suppliers of industrial-grade products offered redundant cabling designs, but these came with an increase in complexity (see Figure 2).

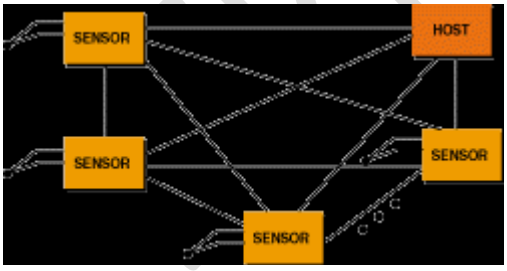


Figure 3. In a web topology, all nodes are potentially connected to all other nodes. Connectivity among a large collection of sensors gets complex because all nodes must have a connection to all other nodes. Some connections can be eliminated by using repeaters and routers to make virtual connections. The World Wide Web is a good example of this topology.

- The promise of the web topology (i.e., when all nodes are connected all the time) had to wait until vendors developed a way to interconnect nodes without the required wiring connections.
- A network of any appreciable size becomes infeasible if all wires must be connected specifically for the network (see Figure 3). Early star topologies were successful as long as the star wasn't too large.
- The World Wide Web illustrates what is possible, though, if you can use wiring that is already in place. The telephone network provides the available connectivity in most parts of the country, although at less than suitable speeds in many locations

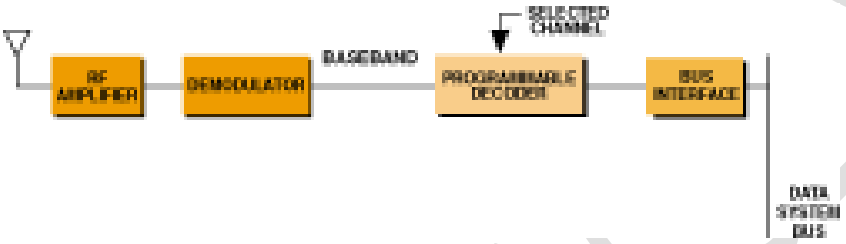


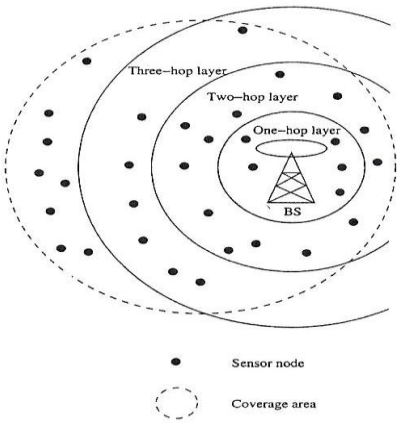
Figure 5. Simultaneous sampling is more difficult with this receiver architecture. The selected channel codes can be stored and stepped through so that each channel's data gets to the data system bus

Applications of WSNs

- Constant monitoring & detection of specific events
- Military, battlefield surveillance
- Forest fire & flood detection
- Habitat exploration of animals
- Patient monitoring
- Home appliances

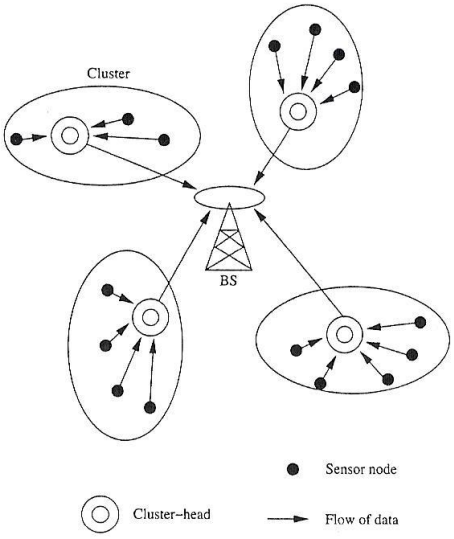
Layered Architecture

- A single powerful base station (BS)
- Layers of sensor nodes around BS
- Layer i: All nodes i-hop away from BS
- Applications:
    - In-building: BS is an access point
    - Military
- Short-distance, low power



Clustered Architecture

- Organizes the sensor nodes into clusters
- Each cluster is governed by a cluster-head
- Only heads send messages to a BS
- Suitable for data fusion
- Self-organizing.



Sensor node architecture

- Main components of a WSN node
  - Controller
  - Communication device(s)
  - Sensors/actuators
  - Memory
  - Power supply
- Main options:
  - Microcontroller – general purpose processor, optimized for embedded applications, low power consumption
  - DSPs – optimized for signal processing tasks, not suitable here
  - FPGAs – may be good for testing
  - ASICs – only when peak performance is needed, no flexibility
- Example microcontrollers
  - Texas Instruments MSP430

- 16-bit RISC core, up to 4 MHz, versions with 2-10 kbytes RAM, several DACs, RT clock, prices start at 0.49 US$

- Atmel ATMega
  - 8-bit controller, larger memory than MSP430, slower.
  -

Sensor network architecture -Introduction

- Sensor networks are highly distributed networks of small, lightweight wireless node, deployed in large numbers to monitor the environment or system.

- Each node of the sensor networks consist of three subsystem:
  - Sensor subsystem: senses the environment
  - Processing subsystem: performs local computations on the sensed data
  - Communication subsystem: responsible for message exchange with neighboring sensor nodes

- The features of sensor nodes
  - Limited sensing region, processing power, energy.

The advantage of sensor networks

  - Robust : a large number of sensors
  - Reliable :
  - Accurate : sensor networks covering a wider region
  - Fault-tolerant : many nodes are sensing the same event
- Two important operations in a sensor networks
  - Data dissemination : the propagation of data/queries throughout the network
  - Data gathering : the collection of observed data from the individual sensor nodes to a sink
- The different types of sensors
  - Seismic, thermal, visual, infrared.

Applications of Sensor Networks

- **Using in military**
  - Battlefield surveillance and monitoring, guidance systems of intelligent missiles, detection of attack by weapons of mass destruction such as chemical, biological, or nuclear

- **Using in nature**
  - Forest fire, flood detection, habitat exploration of animals

- **Using in health**
  - Monitor the patient's heart rate or blood pressure, and sent regularly to alert the concerned doctor, provide patients a greater freedom of movement.
  - Using in home (smart home)
  - Sensor node can built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote-controlled

- **Using in office building**
  - Airflow and temperature of different parts of the building can be automatically controlled

- **Using in warehouse**
  - Improve their inventory control system by installing sensors on the products to track their movement.
  -

Issues and Challenges in Designing a Sensor Network

Issues and Challenges

- Sensor nodes are randomly deployed and hence do not fit into any regular topology. Once deployed, they usually do not require any human intervention. Hence, the setup and maintenance of the network should be entirely autonomous.
- Sensor networks are infrastructure-less. Therefore, all routing and maintenance algorithms need to be distributed.

- ❖ Energy problem
- ❖ Hardware and software should be designed to conserve power
- ❖ Sensor nodes should be able to synchronize with each other in a completely distributed manner, so that TDMA schedules can be imposed.
- ❖ A sensor network should also be capable of adapting to changing connectivity due to the failure of nodes, or new nodes powering up. The routing protocols should be able to dynamically include or avoid sensor nodes in their paths.

Types of sensor networks

Depending on the environment

- terrestrial WSN
  - Ad Hoc (unstructured)
  - Preplanned (structured)
- underground WSN
  - Preplanned
  - more expensive equipment, deployment, maintenance
- underwater WSN
  - fewer sensor nodes(sparse deployment)
  - more expensive than terrestrial
  - acoustic wave communication
    - Limited bandwidth
    - long propagation delay
    - signal fading

- ❖ Depending on the environment
  - multi-media WSN

- sensor nodes equipped with cameras and microphones
- pre-planned to guarantee coverage
- High bandwidth/low energy, QoS, filtering, data processing and compressing techniques

- mobile WSN
  - ability to reposition and organize itself in the network
  - Start with Initial deployment and spread out to gather information
  - deployment, localization, self-organization, navigation and control, coverage, energy, maintenance, data process

Platforms for wireless sensor networks

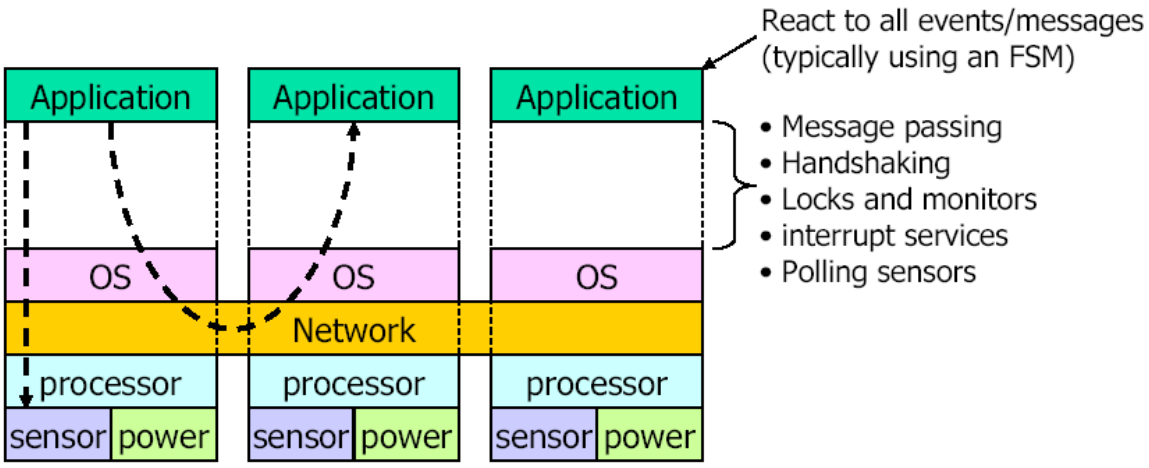
Software Development Infrastructure for Sensor Networks

- **Operating systems (**TinyOS)
- Resource (device) management
  - Basic primitives
  - Protocols (MAC, routing) {covered in many previous lectures}
- Programming languages and runtime environments
  - Low level (C, nesC)
  - Very high level abstractions (Regiment)
- Services needed
  - Synchronization of clocks (RBS)
  - Propagation of new code to all nodes *(Trickle)*
  - Localization

Challenges in programming sensors

- WSN usually has severe power, memory, and bandwidth limitations

- WSN must respond to multiple, concurrent stimuli
- At the speed of changes in monitored phenomena
- WSN are large-scale distributed systems

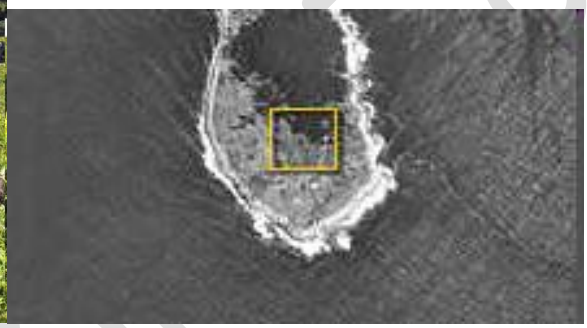


Node-level methodology and platform

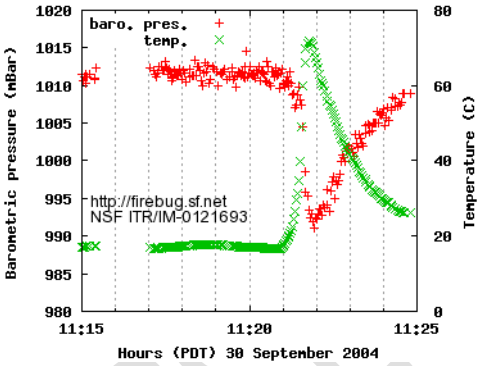
- Traditional design methodologies are node-centric
- Node-level platforms
  - Operating system
    - Abstracts the hardware on a sensor node
    - Provides services for apps such as, traditionally, file management, memory allocation, task scheduling, device drivers, networking…
  - Language platform
    - Provides a library of components to programmers

Applications of wireless sensor networks

- Environmental/Habitat monitoring
- Acoustic detection
- Seismic Detection
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring



- Intel Research Laboratory at Berkeley initiated a collaboration with the College of the Atlantic in Bar Harbor and the University of California at Berkeley to deploy wireless sensor networks on Great Duck Island, Maine (in 2002)
- Monitor the microclimates in and around nesting burrows used by the Leach's Storm Petrel
- Goal : habitat monitoring kit for researchers worldwide



- Wildfire Instrumentation System Using Networked Sensors
- Allows predictive analysis of evolving fire behavior
- Firebugs: GPS-enabled, wireless thermal sensor motes based on TinyOS that self-organize into networks for collecting real time data in wild fire environments
- Software architecture: Several interacting layers (Sensors, Processing of sensor data, Command center

Preventive Maintenance on an Oil Tanker in the North Sea: The BP Experiment

- Collaboration of Intel & BP
- Use of sensor networks to support preventive maintenance on board an oil tanker in the North Sea.

- A sensor network deployment onboard the ship
- System gathered data reliably and recovered from errors when they occurred

RFID

1. The Origins of RFID

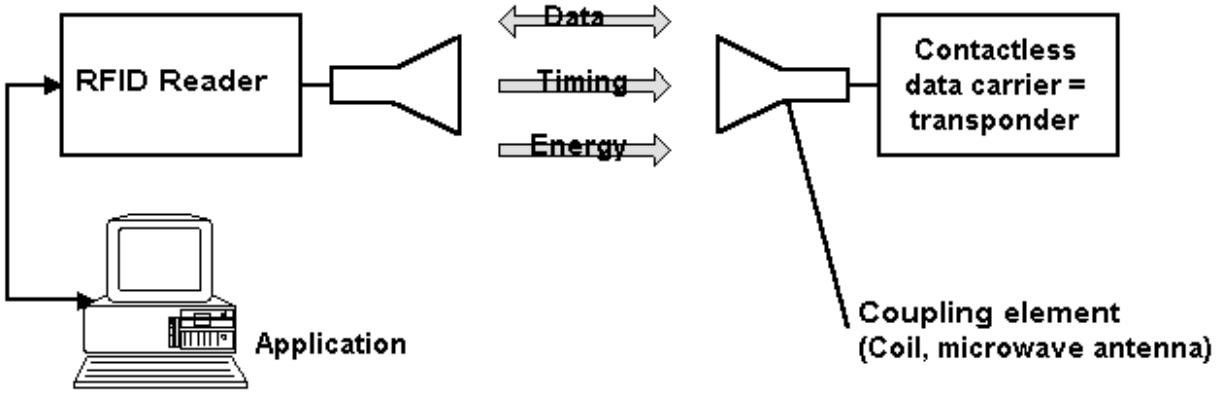
- It was first used over sixty years ago by Britain to identify friend and foe aircraft in World War II and was part of refinement of Radar.
- It was during the Swinging Sixties that RFID started to be looked as a solution for the commercial world. The first commercial applications involving RFID followed during the Seventies and Eighties.
- These commercial applications were concerned with identify some asset inside a single location. They were based on proprietary infrastructures.
- The third era of RFID started in 1998, when researchers at the Massachusetts Institute of Technology (MIT) Auto-ID Centre began to research new ways to track and identify objects as they move between physical locations.

- This research, which has a global outlook, centred on radio frequency technology and how information held on tags can be effectively scanned and shared with business partners in near real time.
- RFID is the reading of physical tags on single products, cases, pallets, or re-usable containers which emit radio signals to be picked up by reader devices.
- These devices and software must be supported by a sophisticated software architecture that enables the collection and distribution of location-based information in near real time.
- The complete RFID picture combines the technology of the tags and readers with access to global standardized databases, ensuring real time access to up to date information about relevant products at any point in the supply chain. A key component to this RFID vision is the EPC Global Network.

Introduction to RFID

- Radio Frequency Identification
- Identification system that consists of chip-based tags and readers
- Data is stored and retrieved remotely using radio waves
    - Onboard sensors
    - Product information

Components of an RFID system



Operation type

- Full and half duplex systems
  - Transponder's response is broadcast when the reader's RF field is switched on
- Sequential procedure
  - Reader's RF field is periodically switched off
  - Loss of power during breaks
  - Need auxiliary capacitors or batteries

Frequencies of operation

- Low frequency

- 30-300 kHz
- Tags need to be closer to the reader
- Poor discrimination

❖ High frequency/radio frequency

- 3-30 MHz
- Tags can be read from relatively greater distances
- Tags can hold more information

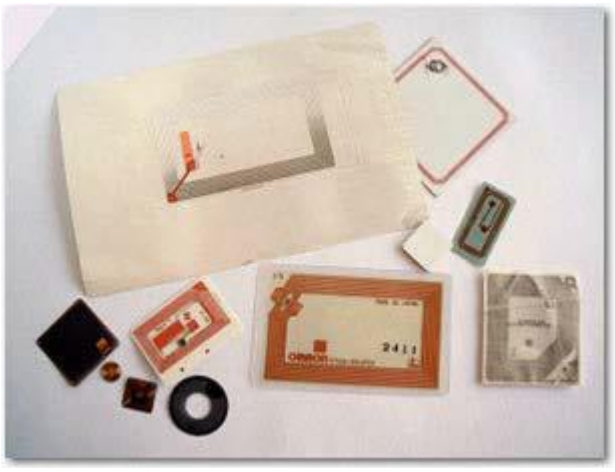
❖ Ultra high frequency/microwave

- >300 MHz
- Longest range
- More interference

RFID Bill of Materials

.

- ❖ **Tag or Transponder** – An RFID tag is a tiny radio device that is also referred to as a transponder, smart tag, smart label or radio barcode.
- ❖ The tag comprises of a simple silicon microchip (typically less than half a millimetre in size) attached to a small flat aerial and mounted on a substrate.
- ❖ The whole device can then be encapsulated in different materials (such as plastic) dependent upon its intended usage.
- ❖ The finished tag can be attached to an object, typically an item, box or pallet and read remotely to ascertain its identity, position or state. For an active tag there will also be a Battery



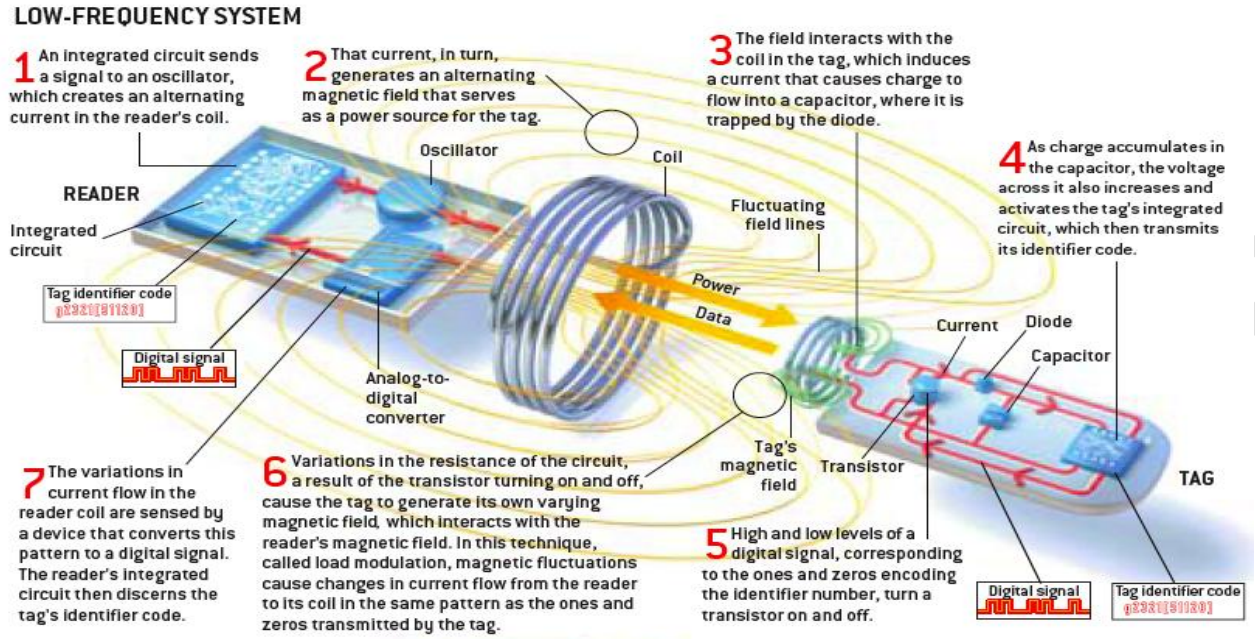
A variety of RFID Tags

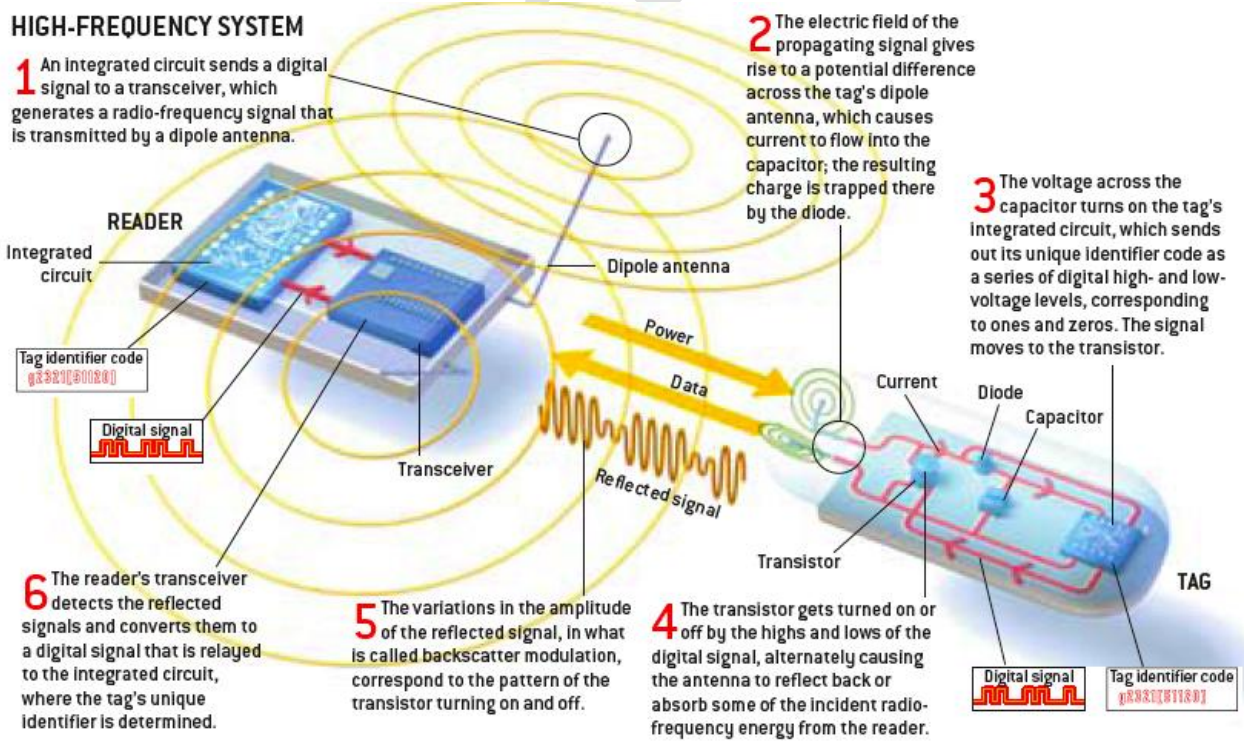
- **Reader or Interrogator** – The reader, sometimes called an interrogator or scanner, sends and receives RF data to and from the tag via antennas.
- A reader may have multiple antennas that are responsible for sending and receiving radio waves

Examples of a Reader with Associated Electronics

- **Host Computer** – The data acquired by the readers is then passed to a host computer, which may run specialist RFID software or middleware to filter the data and route it to the correct application, to be processed into useful information.

- **Technical details**


LOW-FREQUENCY SYSTEM
1 An integrated circuit sends a signal to an oscillator, which creates an alternating current in the reader's coil.
2 That current, in turn, generates an alternating magnetic field that serves as a power source for the tag.
3 The field interacts with the coil in the tag, which induces a current that causes charge to flow into a capacitor, where it is trapped by the diode.
4 As charge accumulates in the capacitor, the voltage across it also increases and activates the tag's integrated circuit, which then transmits its identifier code.
READER
Integrated circuit
Tag identifier code
Digital signal
Oscillator
Coil
Fluctuating field lines
Power
Data
Analog-to-digital converter
Current
Diode
Capacitor
Tag's magnetic field
Transistor
TAG
7 The variations in current flow in the reader coil are sensed by a device that converts this pattern to a digital signal. The reader's integrated circuit then discerns the tag's identifier code.
6 Variations in the resistance of the circuit, a result of the transistor turning on and off, cause the tag to generate its own varying magnetic field, which interacts with the reader's magnetic field. In this technique, called load modulation, magnetic fluctuations cause changes in current flow from the reader to its coil in the same pattern as the ones and zeros transmitted by the tag.
5 High and low levels of a digital signal, corresponding to the ones and zeros encoding the identifier number, turn a transistor on and off.
Digital signal
Tag identifier code


HIGH-FREQUENCY SYSTEM
1 An integrated circuit sends a digital signal to a transceiver, which generates a radio-frequency signal that is transmitted by a dipole antenna.
2 The electric field of the propagating signal gives rise to a potential difference across the tag's dipole antenna, which causes current to flow into the capacitor; the resulting charge is trapped there by the diode.
3 The voltage across the capacitor turns on the tag's integrated circuit, which sends out its unique identifier code as a series of digital high- and low-voltage levels, corresponding to ones and zeros. The signal moves to the transistor.
READER
Integrated circuit
Dipole antenna
Tag identifier code
Digital signal
Transceiver
Power
Data
Reflected signal
Current
Diode
Capacitor
Transistor
TAG
6 The reader's transceiver detects the reflected signals and converts them to a digital signal that is relayed to the integrated circuit, where the tag's unique identifier is determined.
5 The variations in the amplitude of the reflected signal, in what is called backscatter modulation, correspond to the pattern of the transistor turning on and off.
4 The transistor gets turned on or off by the highs and lows of the digital signal, alternately causing the antenna to reflect back or absorb some of the incident radio-frequency energy from the reader.
Digital signal
Tag identifier code

There are two basic types of chips available on RFID tags, Read-Only and Read-Write:

- **Read only chips** are programmed with unique information stored on them during the manufacturing process – often referred to as a 'number plate' application.
- The information on read-only chips can not be changed.
- **With Read-Write chips**, the user can add information to the tag or write over existing information when the tag is within range of the reader. Read-Write chips are more expensive that Read Only chips.
- Applications for these may include field service maintenance or 'item attendant data' – where a maintenance record associated with a mechanical component is stored and updated on a tag attached to the component.
- Another method used is something called a "WORM" chip (Write Once Read Many). It can be written once and then becomes "Read Only" afterwards.

RFID in practice

- To fully understand the capabilities of RFID, it is helpful to consider how the technology can be beneficial in real business situations.
- The following examples illustrate how the technology can impact throughout the supply chain, delivering efficiencies for three types of organisation: manufacturers, distributors and retailers.
- The scenarios focus on a bicycle manufacturer that produces high-end bicycles for the global market. All parts are purchased from vendors, except for the frames, which are made in-house from raw steel pipe.
- The description shows the potential of RFID to deliver benefits at every stage of the supply chain as the bikes are assembled, distributed to retailers and finally sold to customers.

Manufacturing

- The company and all of its suppliers use RFID to share location and other information about the various bicycle parts and subassemblies. This enables vendor managed inventory (VMI) for bicycle components.
- For example, a tyre company supplies the bicycle manufacturer with an in-house stock of tyres. Using VMI, this supplier takes responsibility for stock levels at the bicycle manufacturer, which never has to place an order.

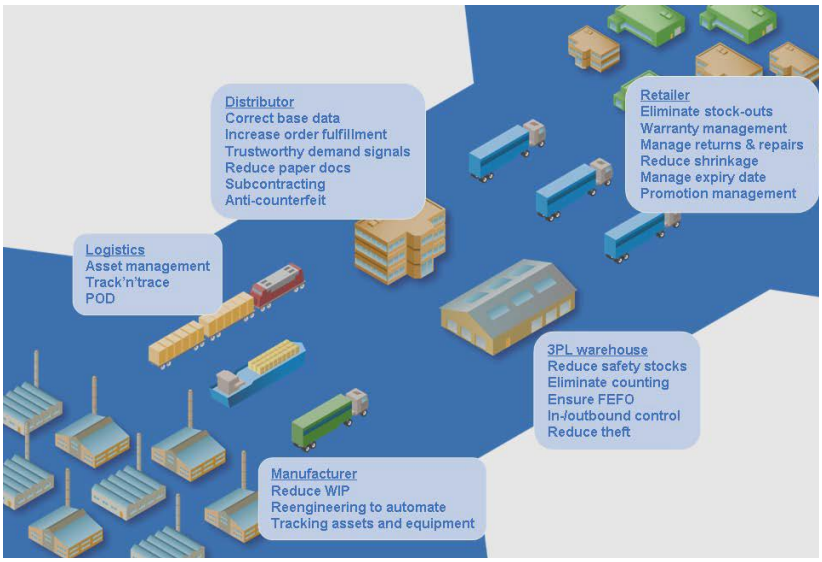
- Each tyre contains an RFID tag that holds product information such as the item and batch number, enabling automated ordering when stocks run low.
- Both companies always know how many tyres are available in the warehouse and react to requirements in real-time.

Scheduling of assembly orders

- Once the bicycle manufacturer has an order of frames ready, it ships them to a paint shop on RFID-tagged pallets containing the production order number and destination.
- The paint shop is equipped with readers that register specific orders when they are delivered. These are then routed to the correct workstations, paint booths or powder coating facilities.
- When the frames have been painted, the system updates tags on the pallets with 'production order complete' status and are then shipped back to the manufacturer.
- When the goods leave the paint shop, the manufacturer is informed when the goods will return. If there were any problems, this information is entered onto the tag, allowing the manufacturer to take appropriate actions.
- RFID readers at the manufacturer recognize the goods when they return from the paint shop. The system automatically notifies the final assembly facility and the order begins.
- Distribution A wholesaler manages the distribution of the manufacturer's bicycles to retailers of all sizes all over the world. This company works with a distributor to deliver a container of bicycles to a retailer.
- The lorry driver unloads the pallets of goods into the warehouse. As the pallets move from the truck into the warehouse, they pass an RFID reader.
- This reader picks up the information about the items received and displays them on a screen next to the doors so the driver can see what has been unloaded.
- Once all the goods are unloaded the trucker confirms that the order is correct and the retailer and distributor systems are updated in real time.

Picking

- Picking at the warehouse is done on an order-by-order basis and the goods are shipped to stores on pallets.
- The pallets carry RFID tags which store the pick list for the order. Because the warehouse handles fulfillment of many sporting goods manufacturers to a number of outlets, the list may contain other items as well as the bicycles.
- As new orders are released in the warehouse they are written to the tag on an empty pallet.
- The next available forklift operator picks up the next empty pallet. The reader on the forklift reads the pick list from the tag on the pallet and displays it on the operator's screen.
- The operator drives to the first location to pick the required items. The system monitors the goods collected, verifies that they are correct and deducts them from the pick list.
- If incorrect goods are collected a warning is triggered. Once the order is complete the operator brings the pallet to the packing area.
- If, for example, the tire manufacturer had a short run of bad tyres, the bicycle manufacturer may need to recall them. In this case, the system would notify the operator when a bike is on the recall list.
- The operator then takes any recalls to a special section of the warehouse, where they are automatically removed from inventory and put on a pallet for return shipment.



Checking the right goods are on the right truck

- Each outbound door has an RFID reader which monitors all pallets that leave the warehouse.
- Once all the pallets that are being shipped have been loaded onto a truck the operator can confirm that this has been done correctly on screen. A warning is triggered if there are any errors.

Store level inventory control

- One of the bicycle manufacturers' customers is an exclusive retailer in the United Kingdom.
- The retailer uses a perpetual SKU-level inventory scenario that tags and tracks items through the receiving process. In the future, it intends to extend this to tagging individual items and tracing them through to the POS.

Receiving

- As soon as an order is despatched from the warehouse, the retailer receives information on when the goods will arrive. When the shipment is unloaded at the back of the store, data is collected from RFID tags attached to each pallet. This is accessed, summarised and compared to the expected shipment.
- Any discrepancies are reported and considered as "shrinkage" until the discrepancy is resolved because the store will be charged for items present in the shipment data.

- Receipts are logged into a store perpetual inventory database. Items that have been recognized are entered into the store inventory records. As a result, systems are updated automatically in real time, increasing the efficiency of their operations and ensuring the accuracy of data by eliminating human error.

Shelf stocking

- As pallets of merchandise are received in the back room, the data is made available to a function for scheduling the stocking process.
- The application is 'aware' of current inventory levels in the store and will schedule stocking of merchandise that is either out-of-stock or at a low inventory level.
- Merchandise that is bulky or difficult to stock is scheduled for delivery when the store is closed or customer traffic is expected to be light. Merchandise is stocked in a sequence that spreads the available stocking labour throughout the store.
- Available store labour resources are taken into account when a shop stocking schedule is produced. The stocking application can present the shop assistant with a shelf stocking list either on a printer or wireless terminal. The shelf stocking work list indicates the location of the merchandise on the pallet as well as indicating a shelf location for merchandise placement.
- When the store assistant indicates that the shelf or rack stocking is complete, an RFID shelf-checker application audits the restocking function and the store shelf inventory levels. Some stores have backroom or secondary stocking areas within a store.
- The stocking function not only includes putting away new merchandise but also moving merchandise from secondary locations to primary selling areas.

Store replenishment and ordering

- In the future, each item of stock will have an RFID tag attached at the point of manufacture. These will enable the store to check its inventory levels quickly and effectively.

- The item-level tags will be able to see discrepancies between the items on the shelves and the store inventory. These could then be noted and reported.
- After checking inventory levels in store, the system will also generate an order and check it against the supply chain for any likely problems.

POS checkout process

Traditionally, all checkouts use barcode scanning. If a local cycling team bought new kit, the shop assistant currently scans the first item and then uses the quantity key to multiply that scan, instead of scanning each item individually.

As a result, the retailer can't collect accurate pricing information or details such as the size and colour of goods sold. To address these issues, the store plans to upgrade its checkout process to include RFID scanning of all products at the POS. This will enable the store to implement an end-to-end automated inventory process.

The proposed system will independently recognise each product sold at the register using RFID for inventory and the barcode for sales.

In addition, goods will be scanned at the POS with no human intervention as they pass within a certain distance of a reader. This makes the checkout process faster for the customer and more efficient for the retailer, who can deploy employees to other, more customer-facing activities

Theft

- The store is also planning a system to deactivate the tags as products leave the store.
- The devices that will disable tags can also potentially be used to determine whether items have been scanned at the POS before they leave the store. In doing so, these will help stores to detect shoplifters and reduce shrinkage accordingly.

Find merchandise in the store

The retailer could also use item-level tags to quickly locate items in the store, thereby increasing operational efficiency and service for the customer. Phone calls and wasted visits to the stock room will no longer be necessary.

Customer loyalty

- The retailer caters to an exclusive clientele of racers and aficionados. As an ultimate goal, it would like to give each customer a store card with an embedded RFID tag.
- Customers who agree to have such a card could be scanned as they enter the store. Those who prefer not to be identified would have a privacy flag next to their details on the database. In this case, nothing would disturb the customer while shopping.
- By tagging loyalty cards, the retailer could potentially harness information on customer shopping history to offer willing customers personalized offers in store.
- To enable this, a shop assistant would have to review customer data once they are identified by the system. The employee could then approach the customer and offer items that may be of interest.
- Eventually, this process could be fully automated, with offers and promotions made to customers' phones or PDAs, through mobile devices mounted on shopping trolleys or through kiosks.
- Item level tagging will mean that each bike sold eventually has a tag containing the date of sale, service plan and repair record.
- This would enable the retailer to effectively manage warrantee agreements and identification of bicycles in the event of theft.

RFID Business Benefits

- Use of RFID technology can increase business productivity and reduce associated costs. To ensure that companies benefit from the advantages RFID provides it is important to understand how to adopt this technology.
- By analyzing current practices and procedures 8 main areas of benefit can be identified. These are:
    - Improved Productivity and Cost Avoidance
    - Decreased Cycle Time and Taking Costs Out

- Reduced Rework
- Reduced Business Risk & Control of Assets
- Improved Security and Service
- Improved Utilization of Resources
- Increased Revenues
- Exception Management

Improved Productivity and Cost Avoidance

❖ Identifying items by RFID involves less work than using barcode scanning and other less automated ways. This leads to greater process effectiveness in many tasks such as receiving and putting away, picking and shipping goods where the time required and cost of identifying items by RFID is substantially less than other methods.

Decreased Cycle Time and Taking Costs Out

❖ RFID scanning is not a serial process, like traditional Barcode scanning, so the business can perform identical tasks much more quickly. This means processes moving goods through a supply chain are more efficient leading to a reduction in the need for larger inventories.

Reduced Rework

❖ As RFID scanning has a greater first time pass accuracy this reduces the number of errors that are generated and retries needed.

Reduced Business Risk & Control of Assets

❖ RFID tagging enables better audit and asset control. The ability to track and trace items better means assets can be located more easily.

❖ The opportunity for enhanced data collection leads to increased accuracy of record keeping and improved asset maintenance. Regulatory compliance can be achieved more effectively.

Improved Security and Service

❖ Being able to validate information relating to an item enables increased security. This individual identification contributes to more effective access control, reductions in shrinkage and other losses and the ability to provide fast

and efficient services at the point of need. Ability to authenticate information can prevent activities like counterfeiting and fraud.

Improved Utilization of Resources

- Information obtained by RFID scanning can be used to improve planning. Processes can be improved, time can be saved, assets can be utilized better.

Increased Revenues

- By eliminating uncertainty companies will suffer less "out of stock" situations and obtain greater item availability, reducing lost sales and increasing choice leading to more sales.

Exception Management

- RFID enables processes and procedures to be measured better. Until a process can be measured accurately it often can't be improved. Decisions that are based on limited, inaccurate, out-of-date information are often poor decisions. The contribution information captured by RFID offers to IT applications will allow managers in companies to be alerted when compensatory business decisions need to be taken.

Applications for RFID

Applications fall into two principal categories: firstly, short range applications where the reader and tag must be in close proximity (such as in access control) and secondly, medium to long application, where the distance may be greater (such as reading across a distribution centre dock door). A sample of applications is shown below:

Access control for people

There are many areas where RFID tags are carried by people to allow them to gain access to facilities or services:

- secure access to work place
- Safety access to dangerous/secure equipment
- Access to a computer or vehicle
- Access to travel on trains/buses
- Access to leisure facilities

Access control for vehicles:

- Secure access on site
- Road tolling
- Instant payment for fuel

Manufacturing automation:

- Control of flexible manufacturing processes by recognizing items being built on a production line (mass customization enabler)
- Labeling key components for later recycling

Logistics and distribution:

- Tracking parcels from shipment to end customer
- Tracking goods from manufacture through to retail

Retail:

- Supply chain management
- Stock taking
- Reducing loss through shrinkage
- Reverse logistics
- Product availability

Maintenance:

- Plant & Equipment
- Fixed assets
- Patients

Product security:

- Tamper evidence
- Product authentication
- Anti-counterfeiting

UNIT IV LOCAL AREA AND WIDE AREA WIRELESS TECHNOLOGIES

IEEE 802.11 technologies – Infrared technologies – Bluetooth networks (OBEX protocol) – Personal area networks – Mobility management – Mobile IP – Establishing wide area wireless networks – Concept and structure of ”Cell” – Call establishment and maintenance – Channel management – Frequency assignment techniques

Definition:

- **Infrared** technology allows computing devices to communicate via short-range wireless signals. With infrared, computers can transfer files and other digital data bidirectional.
- The infrared transmission technology used in computers is similar to that used in consumer product remote control units.

Installation and Usage

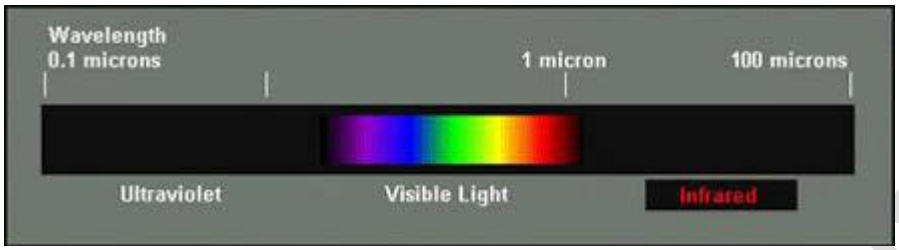
- Computer infrared network adapters both transmit and receive data through ports on the rear or side of a device. Infrared adapters are installed in many laptops and handheld personal devices.
- In Microsoft Windows, infrared connections can be created through the same method as other local area network connections. Infrared networks were designed to support direct two-computer connections only, created temporarily as the need arises.
- However, extensions to infrared technology also support more than two computers and semi-permanent networks.

Range

- Infrared communications span very short distances. Place two infrared devices within a few feet (no more than 5 meters) of each other when networking them.
- Unlike Wi-Fi and Bluetooth technologies, infrared network signals cannot penetrate walls or other obstructions and work only in the direct "line of sight."
- **Performance** - Infrared technology used in local networks exists in three different forms:
    - IrDA-SIR (slow speed) infrared supporting data rates up to 115 Kbps

- IrDA-MIR (medium speed) infrared supporting data rates up to to 4 Mbps

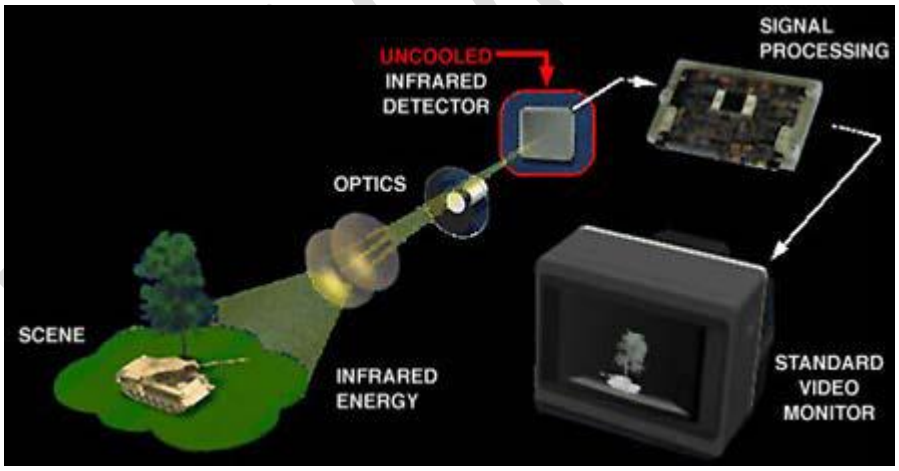
❖ Infrared is an energy similar to visible light, but with a longer wavelength. Infrared energy is invisible to the human eye, however, while visible light energy is emitted by objects only at a very high temperature, infrared energy is emitted by all objects at ordinary temperatures.

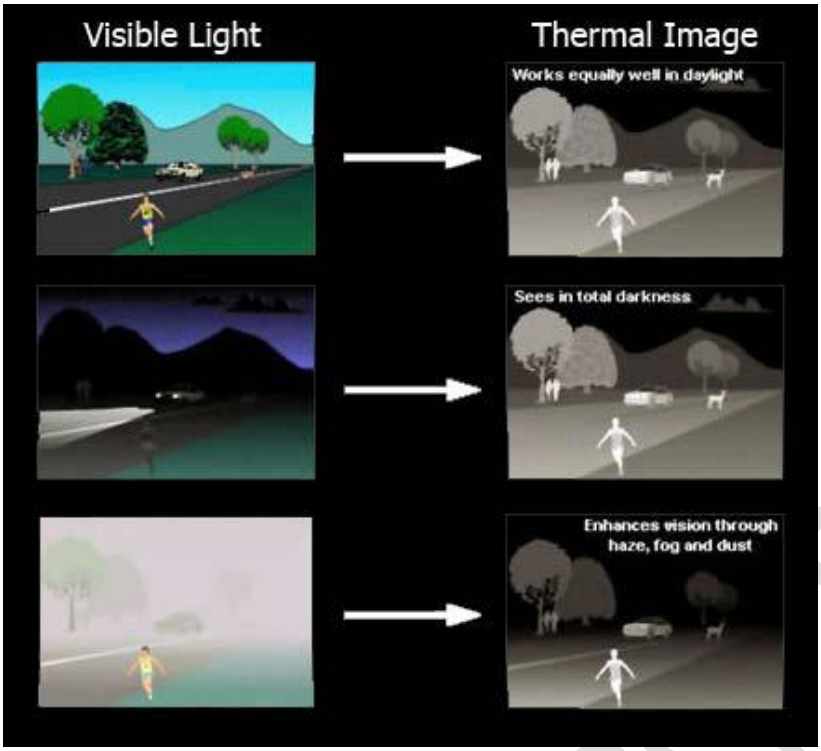


❖ Since thermal imagers' sense infrared energy which varies with the temperature of objects in a scene, the image generated provides a thermal signature of the scene.

❖ This image can be displayed on a standard video monitor. Infrared energy from objects in a scene are focused by optics onto an infrared detector. The infrared information is then passed to sensor electronics for image processing.

❖ The signal processing circuitry translates the infrared detector data into an image that can be viewed on a standard video monitor.





- These systems are affordable and reliable. Thermal imaging systems not only let you see in the dark, but they also enhance your ability to detect critical objects.
- Warmer objects such as people and animals stand out from typically cooler backgrounds. Thermal imaging systems see better than the unaided eye in daylight, night and most poor weather conditions.

Personal Area Network (PAN)

- A Personal Area Network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person.
- The reach of a PAN is typically a few meters. PAN's can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet.

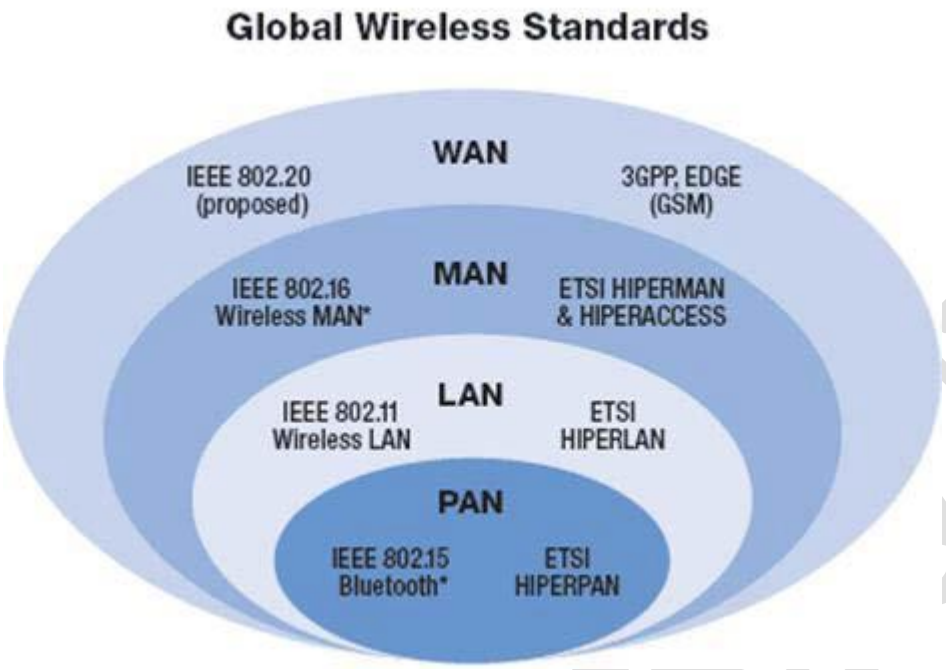
- Personal area networks may be wired with computer buses such as USB and FireWire. However, a Wireless Personal Area Network (WPAN) is made possible with network technologies such as Infrared (IrDA) and Bluetooth.

Bluetooth*:*

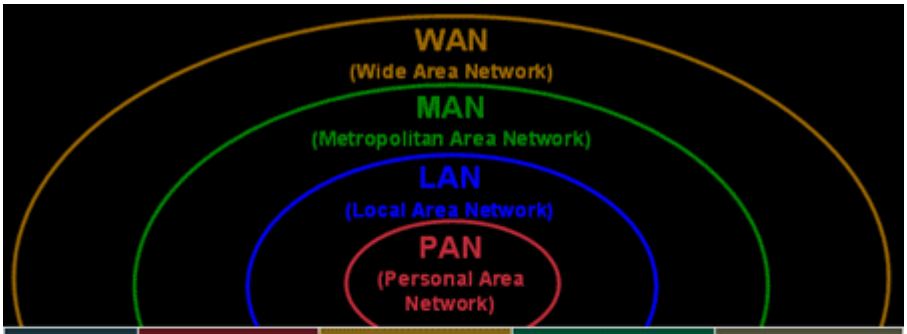
- Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, digital cameras and video game consoles via a secure, globally unlicensed short-range radio frequency.
- Bluetooth is a radio standard and communications protocol primarily designed for low power consumption, with a short range (power class dependent: 1 metre, 10 metres, 100 metres) based around low-cost transceiver microchips in each device.

Infrared (IrDA*)*

The Infrared Data Association (IrDA) defines physical specifications communications protocol standards for the short range exchange of data over infrared light, for typical use in Personal Area Networks.



- These wireless communication technologies evolved over time to enable the transmission of larger amounts of data at greater speeds across a global network. The following figure summaries the technical details of each cluster of technologies.

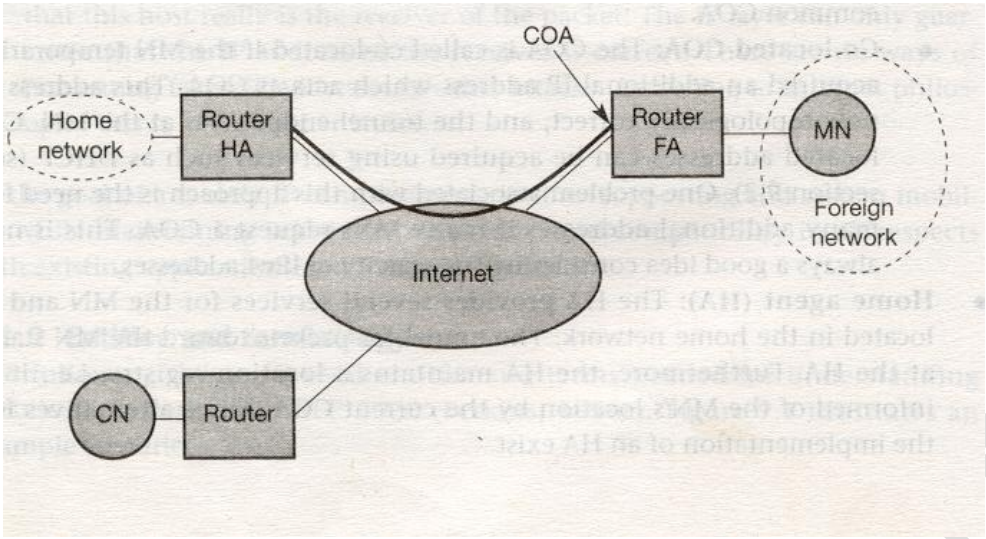


	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11 HiperLAN2	802.11 MMDS, LMDS WiMAX (802.16)	GSM, GPRS, CDMA,HSDPA 2.5-3G-3.5G
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps 1.8/3.6 – 7.2Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	E1 replacement, last mile access	Mobile Phones, cellular data

Mobile IP:

- The purpose of mobile IP is to provide TCP / IP support to the wireless nodes such as laptops and notebooks and even mobile routers (as in the case of airborne routers).
- Wireless nodes have the inherent problem of compatibility, transparency, scalability and efficiency. That is current TCP / IP network structure should not be modified as it has spread allover the globe. Transparency means that mobility should remain invisible to higher application layers.
- That is in spite of lower wireless bandwidth and more discontinuance, the higher layers should work. Enhancing IP for mobility should not generate message flooding as mobile IP provision is likely to lead to with every device implementing mobile IP protocol and hence it needs to be efficient and scalable.

Following diagram indicates the layout of Mobile IP and brief descriptions of these entities is given below.



- **Mobile Node**: MN is the mobile node that can change its point of attachment to the internet using mobile IP. The MN keeps its IP address and can continuously communicate with any other system in the internet as long as link layer connectivity is given.
- **Correspondent Node (CN)**: CN is the node that corresponds with the mobile node. It can be fixed or even mobile. IN the above diagram, it is assumed to be fixed.
- **Home Network:** It is the subnet the MN belongs to with respect to its IP address. NO mobile IP support is needed within its home network.
- **Foreign Network**: It is the current subnet the MN visits and which is not the home network.
- **Foreign Agent (FA):** It is the wired network end point from which the wireless region begins. FAs are routers and form the default routers for the MN. FA can provide the following services:
  - FA address forms the COA (Care Of Address) for the MN node.
  - FA can provide security services to the visiting node.
- **Care Of Address (COA)** COA defines the current location of the MN from an IP point of view. All packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery to the MN from Home Agent (HA) to Foreign Agent (FA) is done using tunneling. COA is the tunnel end point.

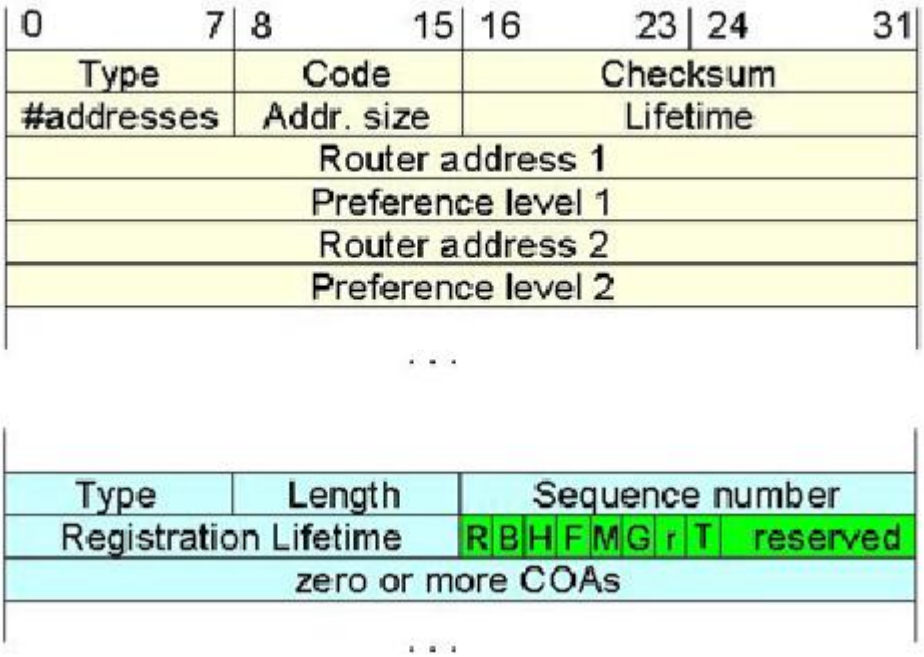
- **Home Agent (HA)** The HA provides several services for the MN and is located in the home network. The tunnel for packets towards the MN starts at the HA. HA maintains location registry that is the current location of MN by the current COA. The HA can be implemented normally on a router.
- **Mobility Agent** : Either a HA or FA are known as mobility agents.

Tunneling:

- As can be seen in the network, a CN, is connected via a router to the internet as are the home network and the foreign networks.
- HA and FA are implemented on the router that are connected to the network. The MN is currently in the foreign network.
- The packets are transferred from the HA to FA in tunneled format and the FA de tunnels the packets and transmit the same to the MN.

Location Discovery:

- The MN is responsible for discovering whether the MN is in a home or foreign network. This process is done by either the Mobile Agent advertisement (HA or FA) or by agent (MN) solicitation.
- Usually, the FA periodically broadcasts the Internet Router Discovery Protocol (IRDP) message in its own network to let the visiting MN know the FA is here and what services it can provide. IN case the MN does not receive this message, it can request the service by sending a solicitation message to inform the FA directly. IF there is no answer, the MN uses DHCP to acquire the new IP address. The mobility agent advertisement packet is shown below:



- The details of the fields are described below:
- The **type** is set 9 for agent advertisement and set to 10 for agent solicitation.
- Code = if the agent is also a router or 16 it is only a Mobile IP agent.
- #Addresses: indicates the number of addresses advertised in this message.
- Address size: The number of 32 bit words of information per each router address.
- Lifetime: Maximum number of seconds that the address is considered valid.
- Router address: The sending routers IP address
- Preference level: Preference levels for each address help a node to choose the router that is the most eager one to get a new node

Mobility Extension:

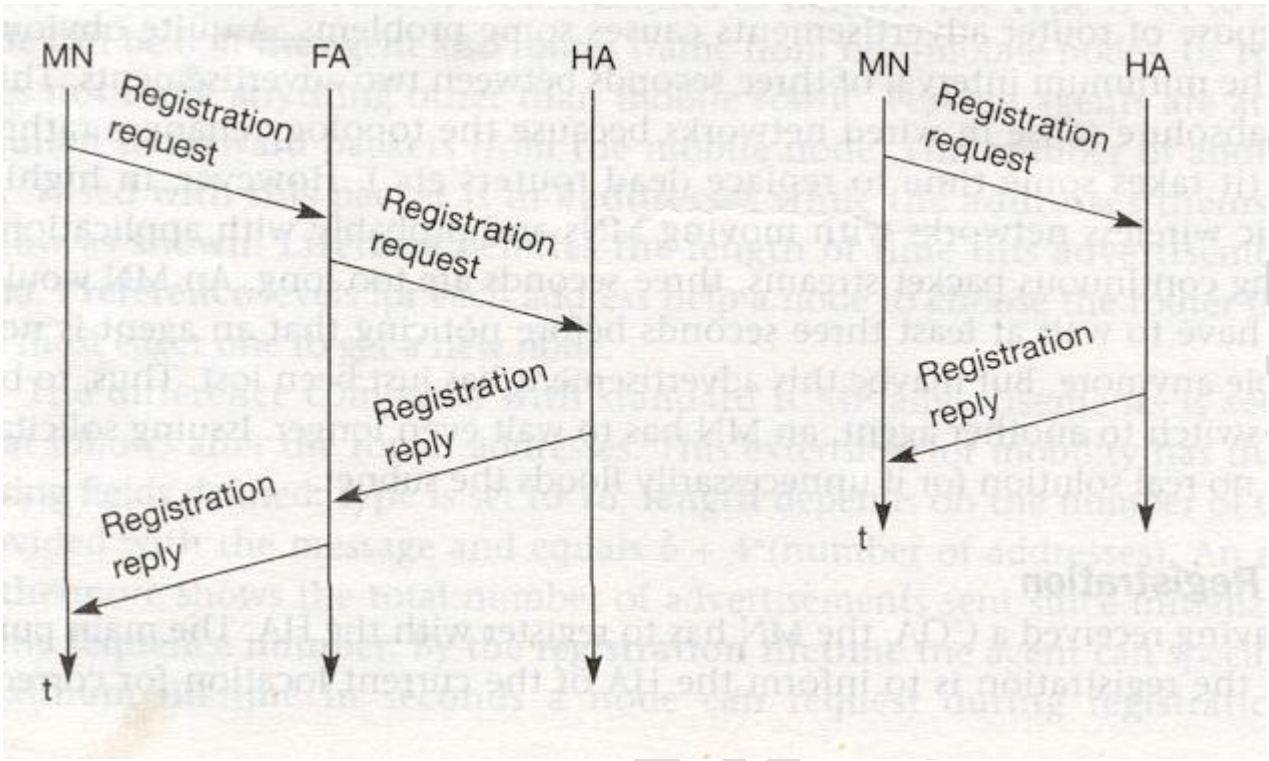
- Type: set to 16. Indicates mobility advertisement extension.
- Length: Depends on the number of COAs provided with the message.
- Sequence Number: Number of Advertisement messages sent since the agent was initialized.

- Registration Lifetime: The longest lifetime in seconds that the registration request will be accepted by this agent.

- Following bits specify the characteristics of an agent in detail:
- R: Indicates whether the registration with this agent is required.
- B: Indicates if the agent is too busy to accept to new registration.
- H / F Indicates if the agent offers services as Home Agent of Foreign Agent.
- M / G: Indicates the type of encapsulation used for the tunnel.
    - (While P-in - P is mandatory, M can specify Minimal and G can specify Generic encapsulation)
- V: indicates the use of header compression.
- A mobile node in a subnet can now receive agent advertisement from either its home agent or a foreign agent. This is
- one way for the MN to discover its location. Other means is by the MN sending DHCP solicitations.

Registration:

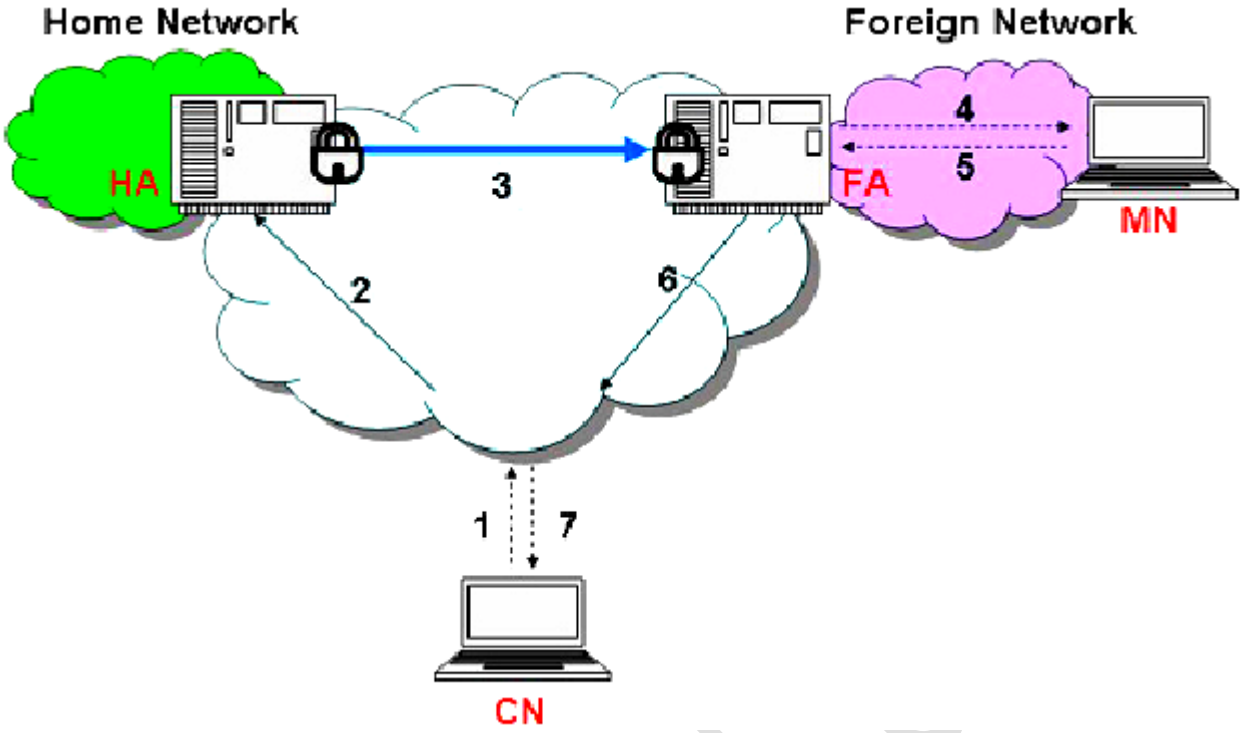
After having received a **COA** The MN has to register with the HA. The main purpose of the registration is to inform the HA of the current location for correct forwarding of the packets. Registration can be done in two different ways depending on the location of COA.



- If the COA is at the FA, registration is done as shown in the diagram.
- The MN sends is registration request containing the COA to the FA which is forwarding the request to the HA. The HA now sets up a mobility binding containing the mobile node's home address and the current COA. Additionally, the mobility binding contains the lifetime of the registration which is negotiated during the registration process.
- Registration expires automatically after the lifetime and is deleted. Therefore, a MN should reregister before expiration. After setting up the mobility bindings, the HA sends a reply message back to the FA which forwards it to the MN.
- If the COA is co located (IN this case, packets are detuned at MA and FA acts as a router), the registration process is simpler as shown in the figure.
- The MN sends the requests directly to the HA and vice versa. This, by the way is also the registration procedure for MNs returning home into their home network. Here they also register directly with the HA.

- After a discovery phase, the MN has to send a registration or deregistration request message with its updated COA back to the HA.
- After that, a registration reply message will be sent back to the MN to confirm the registration process. The HA then updates its mapping address between the home address of the MN and the updated COA.

- In order to deliver packets from the MN to the HA and vice versa, either the FA (with FCOA) or the MN(with CCOA) has to do tunneling to avoid the route propagation problem.
- After the tunnel is established, it is considered as just only one hop end-to-end from either the FA or the MN to the HA. In this regard, the Mobile IP operation is carried out as shown below:
- First, the CN wants to send messages to the MN. It sends IP packets destined for the MN_s home address. These packets will be forwarded to the home network (1 and 2) by normal routing.
- Since the HA knows the MN is not in this network, the HA will intercept these packets.. After that, the HA makes a tunnel (encapsulates the original packets inside a new IP packet), and forwards the packets (3) to the COA (The source IP address is the HA address, and the destination IP address is the COA).
- After taking off the outer header, the FA forwards the packets directly to the MN by link layer address if it is the FCOA (4).
- However, if it is the CCOA, the HA forwards the packets directly to the MN where the packets are deencapsulated. Finally, the MN sends the packets back to the CN as usual



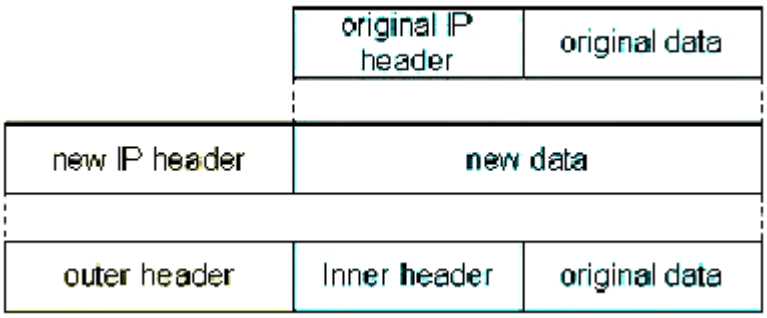
Three kinds of encapsulation technique.

a) IP - in – IP Encapsulation

b) Minimal Encapsulation

c) Generic Routing Encapsulation (GRE)

First, a traditional IP-in-IP encapsulation [RFC 2003, 1996] simply encapsulates the original IP packet within the new IP header as shown below.



IP

- Following figure shows the IP in IP encapsulation. The field of outer header are set as follows:
- Ver: Set to 4 for IP version.
- IHL (Internet Header Length): Indicates the outer header length in 32 bit word length
- TOS (Type of Service): Depends on the reliability, error free and speed of service.
- Length : Includes everything in datagram, data and header count
- IP Identification : To identify to which datagram the newly arrived fragment belongs to
- Flags: 3 individual bits indicate: I bit unused; DF – don't fragment; MF: more fragments
- Fragment offset: Tells where in the current datagram, the fragment belongs
    - TTL(Time to Live): Used to limit the packet life time.
    - IP –in – IP : it is the protocol field and it is set o 4 for IP in IP
    - IP Checksum: Verifies the checksum only.
    - IP Address of HA : It is the source address
- COA : It is the destination address:
- The inner header also will have the same field except for the TTL field which is decremented by 1.
- This means that whole tunnel is considered as one hop although the fragment may be going over a number of routers and other network elements.
- This feature allows the MN to behave as if it were attached to the home network.

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*IP-in-IP*	IP checksum	
IP address of HA			
Care-of address COA			
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	Protocol	IP checksum	
IP address of CN			
IP address of MN			
TCP/UDP/ ... payload			

It can be seen that several header fields are redundant in this encapsulation methods.

Minimal Encapsulation:

The draw backs of minimal encapsulation is addressed in this technique. The technique is shown below:

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	*min. encap.*	IP checksum	
IP address of HA			
care-of address COA			
Protocol	S	reserved	IP checksum
IP address of MN			
original sender IP address (if S=1)			
TCP/UDP/ ... payload			

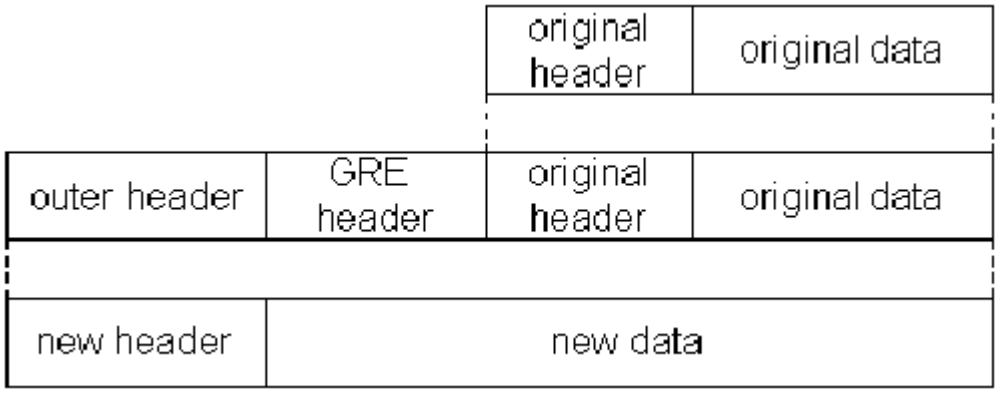
- It is an optional encapsulation method and it is indicated by **min encapsulation** field contains 55 indicating this method. The inner header is different for minimal encapsulation.

- If S bit is set, the original sender address of the CN is included. There is no fragment field which means minimal encapsulation does not work with already fragmented packets.

Generic Routing Encapsulation

While IPinIP and Minimal protocol work for IP, GRE makes provision for encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

The packet of one protocol suite with original header and data is taken and new GRE header is prepended as shown below. Together this forms the new data part or the new packet. Finally, the header of the second protocol suite is put



Following figure shows the fields of a packet inside the tunnel between HA and COA using GRE as encapsulation scheme.

- IN this protocol type in the outer header is 47 (indicated as GRE). Other fields of GRE, such as TTL, TOS may be copied from the original IP header. However, TTL must be decremented by 1 when the packet is decapsulated. The GRE header starts with several flags that indicate if certain fields are present or not.
  - C : IF set, the checksum contains a valid IP checksum of the GRE header and the payload.
  - R : This bit indicates if the offset and routing fields are present and contain valid information.
  - K: If this is set, it indicates the the key fields contains authentication key.

- S: It indicates if sequence number field is present.
- s. It indicates that strict source routing is to be used.

Other fields are:

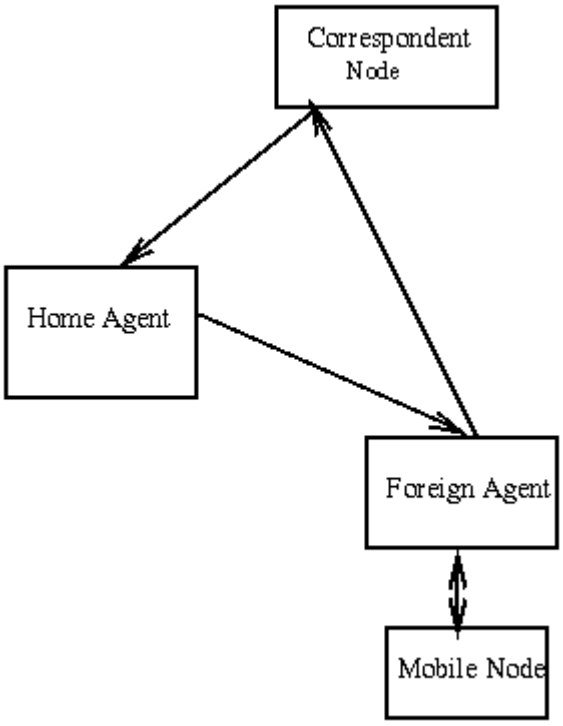
- Rec: This distinguishes GRE from IPinIP and Minimal encapsulation. In that, it represents a counter that shows the number of allowed recursive encapsulation. As soon as the packet arrives at a encapsulator, it checks whether this fields is zero. If this fields is not zero, additional

- encapsulation is allowed. The packet is encapsulated and the field is decremented by one. The default value of this is one, thus allowing only one level of encapsulation.
- Reserved: These fields are ignored.
- Ver: Contains 0 for GRE
- Protocol: Indicates the protocol of the packet following GRE header.
- The standard header of the original packet follows with the source address of the corresponding node

<table>
<tr><td colspan="2">ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">GRE</td><td>IP checksum</td></tr>
<tr><td colspan="5">IP address of HA</td></tr>
<tr><td colspan="5">Care-of address COA</td></tr>
<tr><td>C</td><td>R</td><td>K</td><td>S</td><td>s</td><td>rec.</td><td>rsv.</td><td>ver.</td><td colspan="2">protocol</td></tr>
<tr><td colspan="4">checksum (optional)</td><td colspan="2">offset (optional)</td></tr>
<tr><td colspan="6">key (optional)</td></tr>
<tr><td colspan="6">sequence number (optional)</td></tr>
<tr><td colspan="6">routing (optional)</td></tr>
<tr><td colspan="2">ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">Protocol</td><td>IP checksum</td></tr>
<tr><td colspan="5">IP address of CN</td></tr>
<tr><td colspan="5">IP address of MN</td></tr>
<tr><td colspan="5">TCP/UDP/ ... payload</td></tr>
</table>

Triangular routing

- Consider a situation, when two devices (may be one mobile and one fixed) are located in such a way that the mobile node is closed to fixed node. However, the HA for the mobile node is far off and if the CN wants to communicate with its MN it does in the following way.

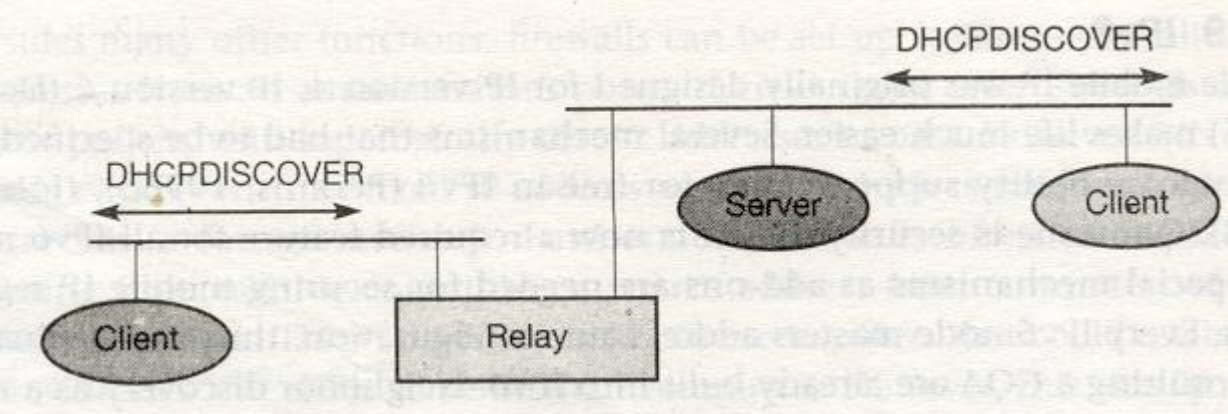


- CN corresponds to HA. HA transmits the data by tunneling to FA as it knows that the MN is at the given COA of FA. And the Foreign Agent delivers the data to MN. Although the nodes are quite closer, may be few meters away, still the data needs to be routed around the world.
- This inefficient behaviour is known as Triangular Routing **.**It is made of CN to HA, HA to COA/MN and MN back to CN. This procedure can cause unnecessary overhead for the network between CN and MN and also increase the latency.
- One way to optimize the route is to inform the CN of the current location of the MN. This is done with the help of four additional messages – binding request, binding update, binding acknowledgement and binding warning.

- These message help CN to store the mobility binding This helps the CN to send its data directly to the current FA. Encapsulation is done now by the CN instead of HA.

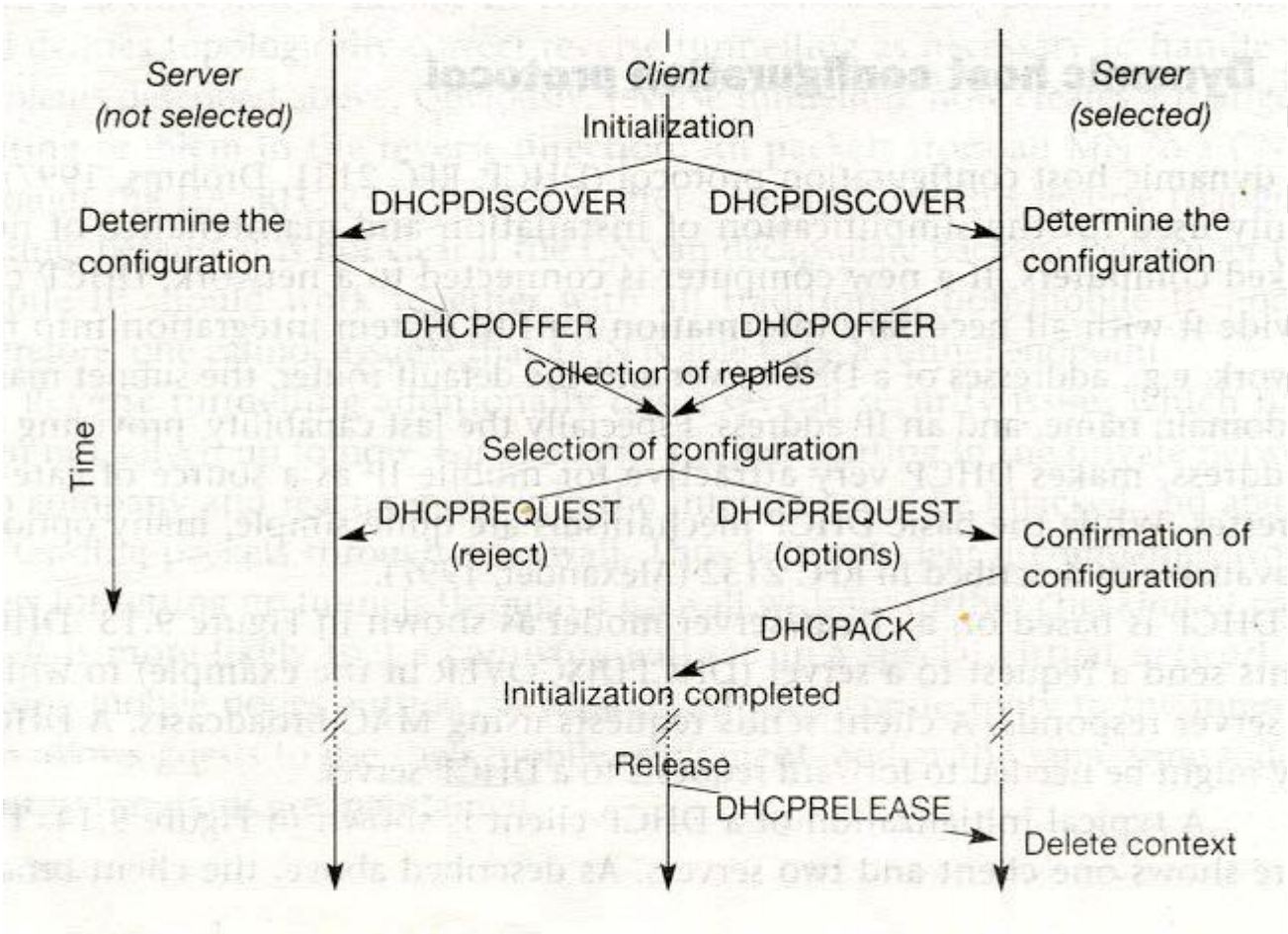
DHCP

- Dynamic Host Configuration Protocol is mainly used network system integration details such as address of DNS server, default router, subnet mask, domain name and IP address DHCP is based on client and server model as shown below:



- DHCP client sends a request to a server (DHCPDISCOVER) to which the server responds.
- The client sends the request using MAC broadcasts. A DHCP relay might be needed in some cases if the server is not near. Following figures shows the initialization and the reply.
- Below figure shows the process for a single client and two servers. Both the servers receive the DHCPDISCOVER broadcast and determine the configuration they can offer to the client.

- The server replies with DHCPOFFER and a list of configuration parameters. Now the client can choose one of the offered configurations.
- The client replies for acceptance as well as for rejection to the servers as shown with DHCPREQUEST (accept) and DHCPREQUEST (reject) respectively.
- Accepting server replies back with DHCPACK and other server release the resources that were reserved initially.
- DHCP is a good method for acquiring the COA for mobile nodes. The DHCP can provide the address of the default router, DNS server, the time server etc.
- IT requires a that DHCP server should be located in the subnet of the Access Point of the mobile node or at least DHCP relay should be provided for forwarding the messages.

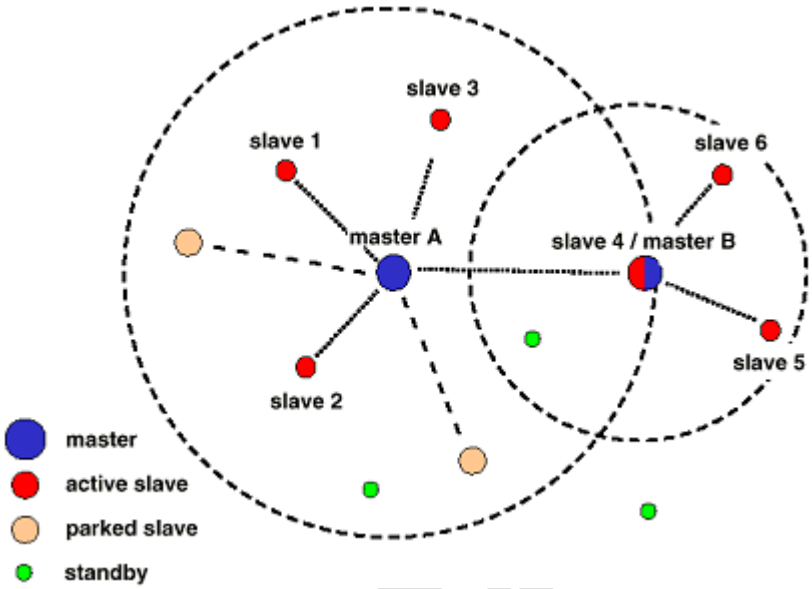


BLUETOOTH PROTOCOL

Basic Concept: the Piconet

- The physical links are created on the basis of masters/slaves (function of the type point to multiple point), a master can
- control up to seven slaves in his zone.
- These form a small network called Piconet.
- The master is simply the first apparatus connected and is the one that sets the clock, the frequency jumping sequence and the access code for the link.
- All the Bluetooth modules of the same Piconet use the same frequency jumping sequence and are synchronized with the master's clock.

- Whatever happens, the machine's role (master or slave) is invisible to the user.
- Also, one apparatus can participate in several piconets, being the slave in one and master in another. The interlacing of several piconets forms what is called a Scatternet. Thanks to the frequency jumping, 10 independent piconets (or up to 80 apparatus) can transmit at maximum output. Above that, the network becomes saturated.

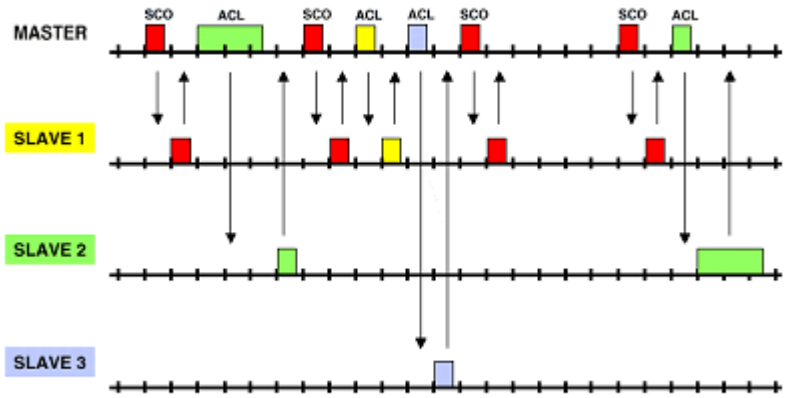


- The transmission diagram of the centre of one piconet is based on the principle of Time Division Duplex (TDD). At first it is the master who sends a packet at a frequency f(k), the slave to whom this packet is addressed (and only this one) has the right to reply to it in the time interval following the arrival of the master packet. The reply from the slave is then given on the frequency channel f(k+1).
- On reception of a master packet, a synchronizations word on the top of it enables the slave to re-synchronises his clock.

Different types of physical channels

Two types of connections are possible:

- Synchronous Connection Orientated (SCO)
- Asynchronous Connection Less (ACL).
- The SCO (Synchronous Connection Oriented) channels are used for voice transfer by reserving slots, they are symmetric between the master and a slave.
- There is a maximum of three in a piconet, a slave being able to control two originating from different masters. One can use the voice packets or the mixed voice/data packets.
- An ACL (Asynchronous Connection Less) channel supplies an asynchronous access between master and slave (a single channel per couple), with the slot as base.
- The data packets only are used. In addition, a slave can only transmit after having received a packet from the master (the following slot). For this purpose, the master can send polling packets to the slaves (when there is nothing more asynchronous to transmit).



The low consumption management modes

- One of Bluetooth's specific characteristics is the low consumption management modes. We will describe here the different modes provided in the Bluetooth norm and how they are used in the case of the bar code reader developed by baracoda.

Active Mode

- In this mode, the Bluetooth module participates actively on the transmission channel.
- The master regularly sends a packet to the slaves (polling) to enable the slaves to be able to send a packet to the master and re-synchronise themselves.
- In this type of mode, the consumption of a Bluetooth module (in transmission) is around 40mA to 50mA (depending on the transmission output).

Sniff Mode

- This is a low consumption mode. A Bluetooth module in the Sniff mode stays synchronised in the piconet. It listens to the piconet at regular intervals (Tsniff) for a short instant.
- This enables it to re-synchronise itself with the piconet and to be able to make use of this Sniff window to send or receive data. The consumption is as low as the Tsniff is large (compared to the Sniff window).
- If Tsniff is in the region of a second and the duration of Sniff (Twin) is in the region of several ms, the consumption will be about 1 to 5% of the maximum transmission consumption. (average consumption of 1mA to 5mA approximately).
- The Baracoda reader generally maintains the connection between 2 consecutive scans. However, for reasons of consumption, the scanner puts itself into the Sniffmode;
- Tsniff is regularly re-negotiated between the scanner and the terminal in such a way that the Tsniff increases as the time without a scan passes.

- The advantage of a large Tsniff is the low consumption and the inconvenience is the delay in sending the bar code. The algorithm developed by Baracoda allows the definition of the best Tsniff, a compromise between low consumption and short delay.

This compromise adapts itself to the user (scan statistic). The advantage in maintaining the connection is to avoid a Paging / Create Connection phase which is responsible for high energy consumption.

Hold Mode

- The module remains synchronized. This is lower consumption mode than the Sniff mode. Only the counter on the Bluetooth chip in hold mode is active. At the end of the Hold period, the Bluetooth module returns to the active mode.

Park Mode :

- A Bluetooth module in this mode is no longer an active member of the piconet. However, it remains synchronised with the master and can listen to a broadcast channel (Beacon Channel).

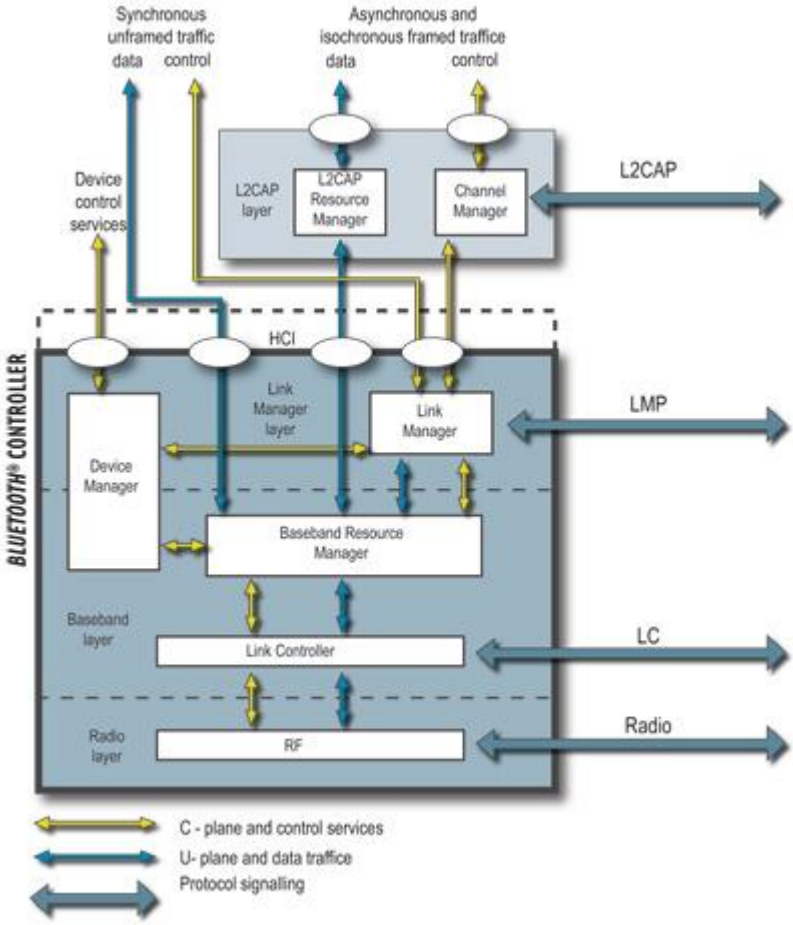
Bluetooth's security system

- The Bluetooth protocol allows the authentication and encryption of a link at the same time. The security is controlled by the lower layers of the Bluetooth protocol.
- A first security level is assured by the fact that each Bluetooth module has a unique address MAC (48-bits). In this way, when the Baracoda scanner connects itself to a terminal with which it is twinned, the bar code is transmitted to this equipment only.
- To achieve a real level of security, the system, the Bluetooth system necessitates 2 secret keys (authentication key and encryption key) as well as a random number (generated regularly).

- **1st stage:** Authentication. The scanner sends a challenge to the terminal with which it wishes to connect itself and sends the decoded bar code. The terminal has to reply to the challenge by returning a link key shared between the scanner and the terminal.
- **2nd stage:** Encryption. When the authentication has been carried out between the 2 devices, the link can be encrypted.

Core System Definition

- The Bluetooth core system covers the four lowest layers and associated protocols defined by the *Bluetooth* specification as well as one common service layer protocol, the service discovery protocol (SDP) and the overall profile requirements are specified in the generic access profile (GAP).
- A complete Bluetooth application requires a number of additional services and higher layer protocols that are defined in the Bluetooth specification.



Bluetooth Controller

- The lowest three layers are sometimes grouped into a subsystem known as the *Bluetooth* controller.
- This is a common implementation involving a standard physical communications interface between the *Bluetooth* controller and remainder of the Bluetooth system including the

- L2CAP, service layers and higher layers (known as the *Bluetooth* host). Although this interface is optional, the architecture is designed to allow for its existence and characteristics. The *Bluetooth* specification enables interoperability between independent
  Bluetooth enabled systems by defining the protocol messages exchanged between equivalent layers, and also interoperability between independent Bluetooth sub-systems by defining a common interface between *Bluetooth* controllers and *Bluetooth* hosts.

- A number of functional blocks are shown and the path of services and data between these. The functional blocks shown in the diagram are informative; in general the *Bluetooth* specification does not define the details of implementations except where this is required for interoperability.

Core System Protocols and Signaling

- Standard interactions are defined for all inter-device operation, where *Bluetooth* devices exchange protocol signaling according to the *Bluetooth* specification.

- The *Bluetooth* core system protocols are the radio (RF) protocol, link control (LC) protocol, link manager (LM) protocol and logical link control and adaptation protocol (L2CAP), all of which are fully defined in subsequent parts of the *Bluetooth* specification.

- In addition, the service discovery protocol (SDP) is a service layer protocol required by all *Bluetooth* applications.

- The Bluetooth core system offers services through a number of service access points that are shown in the diagram as ellipses. These services consist of the basic primitives that control the *Bluetooth* core system.

- The services can be split into three types. There are device control services that modify the behavior and modes of a *Bluetooth* device, transport control services that create, modify and release traffic bearers (channels and links), and data services that are used to submit data for transmission over traffic bearers.

- It is common to consider the first two as belonging to the C-plane and the last as belonging to the U-plane.

Host to Controller Interface (HCI): Splits Bluetooth Stack Into Controller and Host

A service interface to the *Bluetooth* controller sub-system is defined such that the *Bluetooth* controller may be considered a standard part.

- In this configuration the *Bluetooth* controller operates the lowest three layers and the L2CAP layer is contained with the rest of the *Bluetooth* application in a host system.
- The standard interface is called the host to controller interface (HCI). Implementation of this standard service interface is optional.
- As the *Bluetooth* architecture is defined with the possibility of a separate host and controller communicating through an HCI, a number of general assumptions are made.
- The *Bluetooth* controller is assumed to have limited data buffering capabilities in comparison with the host. Therefore the L2CAP layer is expected to carry out some simple resource management when submitting L2CAP PDUs to the controller for transport to a peer device.
- This includes segmentation of L2CAP SDUs into more manageable PDUs and then the fragmentation of PDUs into start and continuation packets of a size suitable for the controller buffers, and management of the use of controller buffers to ensure availability for channels with quality of service (QoS) commitments.

Error Detection in L2CAP Layer

- The baseband layer provides the basic ARQ protocol in *Bluetooth* technology. The L2CAP layer can optionally provide a further error detection and retransmission to the L2CAP PDUs.
- This feature is recommended for applications with requirements for a low probability of undetected errors in the user data. A further optional feature of L2CAP is a window-based flow control that can be used to manage buffer allocation in the receiving device. Both of these optional features augment the QoS performance in certain scenarios.
- Although these assumptions may not be required for embedded *Bluetooth* technology implementations that combine all layers in a single system, the general architectural and QoS models are defined with these assumptions in mind, in effect a lowest common denominator.

Testing Interfaces: RF and Test Control Interface (TCI)

- Automated conformance testing of implementations of the *Bluetooth* core system is required. This is achieved by allowing the tester to control the implementation through the RF interface, which is common to all *Bluetooth* systems, and through the test control interface (TCI), which is only required for conformance testing.
- The tester uses exchanges with the implementation under test (IUT) through the RF interface to ensure the correct responses to requests from remote devices.
- The tester controls the IUT through the TCI to cause the IUT to originate exchanges through the RF interface so that these can also be verified as conformant.
- The TCI uses a different command-set (service interface) for the testing of each architectural layer and protocol. A subset of the HCI command-set issued as the TCI service interface for each of the layers and protocols within the *Bluetooth* controller subsystem.
- A separate service interface is used for testing the L2CAP layer and protocol. As an L2CAP service interface is not defined in the *Bluetooth* core specification it is defined separately in the TCI specification. Implementation of the L2CAP service interface is only required for conformance testing.

Core Architecture Blocks

Channel Manager

- The channel manager is responsible for creating, managing, and destroying L2CAP channels for the transport of service protocols and application data streams.
- The channel manager uses the L2CAP protocol to interact with a channel manager on a remote (peer) device to create these L2CAP channels and connect their endpoints to the appropriate entities.
- The channel manager interacts with its local link manager to create new logical links (if necessary) and to configure these links to provide the required QoS for the type of data being transported.

L2CAP Resource Manager

- The L2CAP resource manager block is responsible for managing the ordering of submission of PDU fragments to the baseband and some relative scheduling between channels to ensure that L2CAP channels with QoS commitments are not denied access to the physical channel due to *Bluetooth* controller resource exhaustion.
- This is required because the architectural model does not assume that the *Bluetooth* controller has limitless buffering, or that the HCI is a pipe of infinite bandwidth. L2CAP resource managers may also carry out traffic conformance policing to ensure that applications are submitting L2CAP SDUs within the bounds of their negotiated QoS settings.
- The general *Bluetooth* data transport model assumes well-behaved applications, and does not define how an implementation is expected to deal with this problem.

Device Manager

- The device manager is the functional block in the baseband that controls the general behavior of the *Bluetooth* enabled device.
- It is responsible for all operation of the *Bluetooth* system that is not directly related to data transport, such as inquiring for the presence of other nearby *Bluetooth* enabled devices, connecting to other *Bluetooth* enabled devices or making the local *Bluetooth* enabled device discoverable or connectable by other devices.
- The device manager requests access to the transport medium from the baseband resource controller in order to carry out its functions.
- The device manager also controls local device behavior implied by a number of the HCI commands, such as managing the device local name, any stored link keys, and other functionality.

Link Manager

- The link manager is responsible for the creation, modification, and release of logical links (and, if required, their associated logical transports), as well as the update of parameters related to physical links between devices.
- The link manager achieves this by communicating with the link manager in remote *Bluetooth* devices using the link management protocol (LMP).

- The LMP allows the creation of new logical links and logical transports between devices when required, as well as the general control of link and transport attributes such as the enabling of encryption on the logical transport, the adapting of transmit power on the physical link or the adjustment of QoS settings for a logical link.

Baseband Resource Manager

The baseband resource manager is responsible for all access to the radio medium. It has two main functions.

At its heart is a scheduler that grants time on the physical channels to all of the entities that have negotiated an access contract. The other main function is to negotiate access contracts with these entities.

- An access contract is effectively a commitment to deliver a certain QoS that is required in order to provide a user application with an expected performance.
- The access contract and scheduling function must take account of any behavior that requires use of the *Bluetooth* radio.
- This includes, for example, the normal exchange of data between connected devices over logical links and logical transports, as well as the use of the radio medium to carry out inquiries, make connections, be discoverable or connectable, or to take readings from unused carriers during the use of AFH mode.
- In some cases the scheduling of a logical link results in changing to a different physical channel from the one that was previously used.
- This may be, for example, due to involvement in scatternet, a periodic inquiry function, or page scanning. When the physical channels are not time slot aligned, then the resource manager also accounts for the realignment time between slots on the original physical channel and slots on the new physical channel.
- In some cases the slots will be naturally aligned due to the same device clock being used as a reference for both physical channels.

Link Controller

- The link controller is responsible for the encoding and decoding of *Bluetooth* packets from the data payload and parameters related to the physical channel, logical transport and logical link.

- The link controller carries out the link control protocol signaling (in close conjunction with the scheduling function of the resource manager), which is used to communicate flow control and acknowledgement and retransmission request signals.
- The interpretation of these signals is a characteristic of the logical transport associated with the baseband packet. Interpretation and control of the link control signaling is normally associated with the resource manager's scheduler.

RF

- The RF block is responsible for transmitting and receiving packets of information on the physical channel. A control path between the baseband and the RF block allows the baseband block to control the timing and frequency carrier of the RF block. The RF block transforms a stream of data to and from the physical channel and the baseband into required formats.

UNIT V PROTOCOLS AND APPLICATIONS

Networking protocols – Packet switched protocols – Routing protocols for sensor networks – Data centric protocols – Hierarchical protocols – Location – Based protocols – Multimedia Messaging Service (MMS) protocols – Wireless Application Protocol (WAP) – Applications of pervasive computing – Retail – Healthcare – Sales force automation – Tracking applications.

Introduction to Network Protocols

- A protocol is a set of rules and conventions for sending information over a network.
- Protocols can be added or deleted at will and selectively bound to all network interfaces.
- Binding order is determined by the order in which the protocols were initially installed.
- Binding order can be changed at any time on a per-interface basis.
- Network services can be selectively enabled or disabled on a per-adapter or per-protocol basis.
- Transmission Control Protocol/Internet Protocol (TCP/IP)
- Asynchronous Transfer Mode (ATM)
- NWLink
- NetBIOS Enhanced User Interface (NetBEUI)

- AppleTalk
- Data Link Control (DLC)
- Infrared Data Association (IrDA)

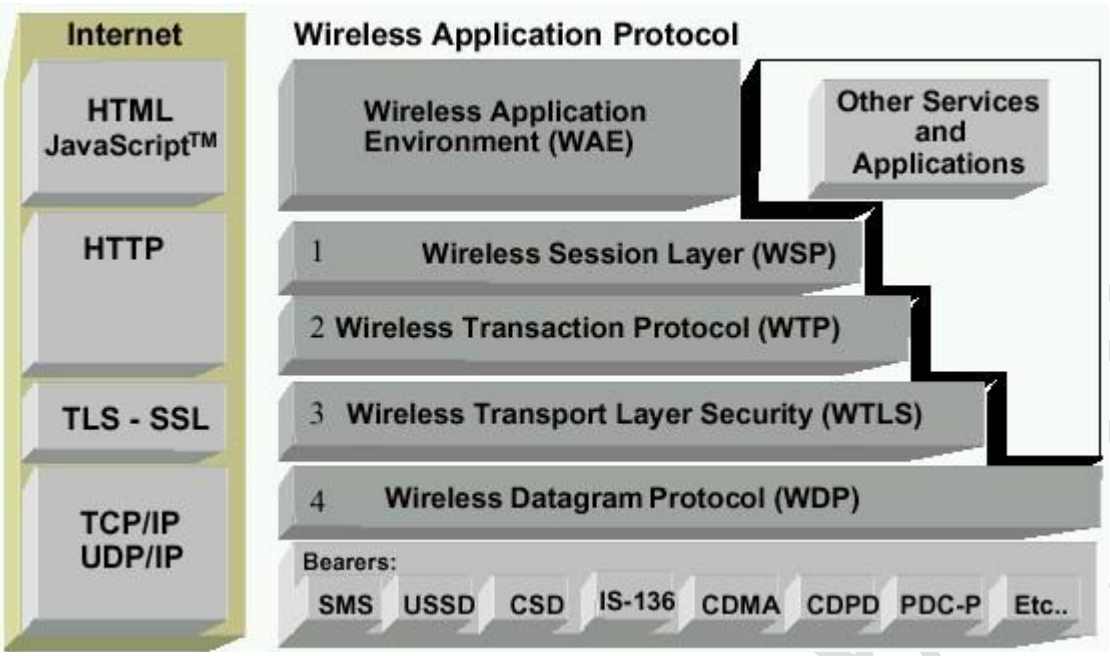
TCP/IP

- The TCP/IP suite has been adopted by Microsoft as the strategic enterprise transport protocol for Microsoft Windows 2000.
- The Windows 2000 TCP/IP suite is designed to make it easy to integrate Microsoft enterprise networks into large-scale corporate, government, and public networks.

WIRELESS APPLICATION ENVIRONEMNT

- The purpose of the WAE is to create a general purpose application environment based mainly on existing technologies of the WWW.
- This should allow service providers, software manufacturers or hardware vendors to integrate their application so that they can reach wide variety of different wireless platforms in an efficient way.
- Some of the features of the Wireless Application Environment are given below:
    - Device and network independent application environment
    - Designed for low-bandwidth, wireless devices
    - Considerations of slow links, limited memory, low computing power, small display, simple user interface (compared to desktops)
    - Integrated Internet/WWW programming model
    - High interoperability

WAP Architecture:

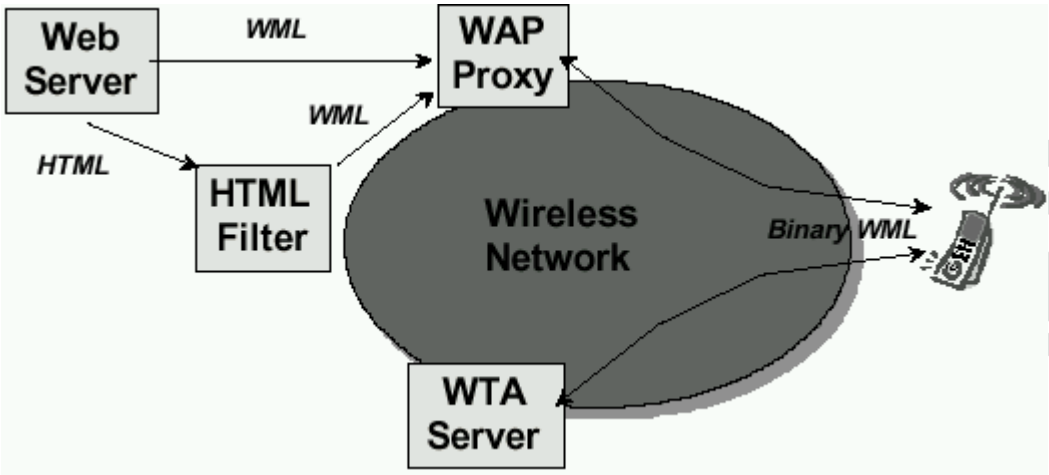


- Wireless Application Environment Specifies
  - WML Microbrowser
  - WMLScript Virtual Machine
  - WMLScript Standard Library
  - Wireless Telephony Application Interface (WTAI)
  - WAP content types .
- Transmission of data is carried out by different **bearer services.** WAP does not specify bearer services, but uses existing data services.
- Examples are SMS of GSM, circuit switched data of HSCSD (High Speed Circuit Switched Data) in GSM, or packet switched data such as GPRS or any other bearer services such as IS 136, CDMA etc.
- **Brief details are given below:**
- WAE (Wireless Application Environment): – Architecture: application model, browser, gateway, server
- WML: XML-Syntax, based on card stacks, variables, ...
- WTA: telephone services, such as call control, phone book etc.
- WSP (Wireless Session Protocol): – Provides HTTP 1.1 functionality
- Supports session management, security, etc.

- WTP (Wireless Transaction Protocol): – Provides reliable message transfer mechanisms
- Based on ideas from TCP/RPC

- WTLS (Wireless Transport Layer Security): – Provides data integrity, privacy, authentication functions.Based on ideas from TLS/SSL
- WDP (Wireless Datagram Protocol): – Provides transport layer functions
- WAE components:
- Architecture –Application model, Micro Browser, Gateway, Server
- User Agents : –WML/WTA/Others
    - –content formats: vCard, vCalender, Wireless Bitmap, WML.
- WML : –XML-Syntax, based on card stacks, variables,
- WMLScript : –procedural, loops, conditions, ... (similar to JavaScript)
- WTA : –telephone services, such as call control, text messages, phone book, ... (accessible from WML/WMLScript)
- Proxy (Method/Push)

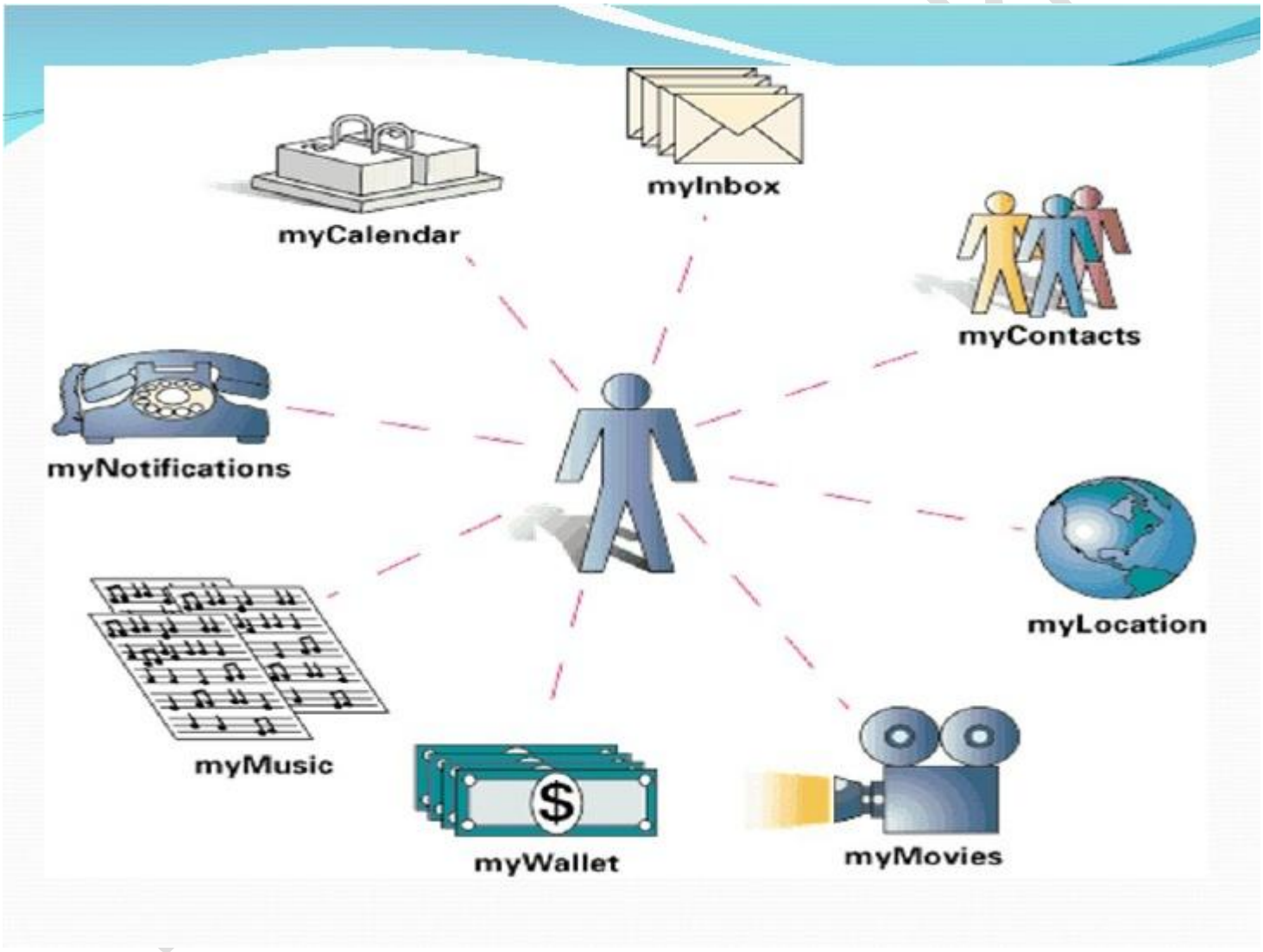
WAP architecture



- In the example, the WAP client communicates with two servers in the wireless network.
- The WAP proxy translates WAP requests to WWW requests thereby allowing the WAP client to submit requests to the web server. The proxy also encodes the responses from the web server into the compact binary format understood by the client.
- If the web server provides WAP content (e.g., WML), the WAP proxy retrieves it directly from the web server. However, if the web server provides WWW content (such as HTML), a filter is used to translate the WWW content into WAP content.
- For example, the HTML filter would translate HTML into WML. The Wireless Telephony Application (WTA) server is an example origin or gateway server that responds to requests from the WAP client directly. The WTA server is used to provide WAP access to features of the wireless network provider's telecommunications infrastructure.

Applications of pervasive computing

Pervasive computing systems outside the laboratory poses significant challenges and in the case of retail, requires the deployment of new infrastructure, primarily broadband wireless connectivity for mobile devices inside the store and electronically tagged grocery products with unique identifiers following a global classification scheme.


myCalendar
myInbox
myContacts
myNotifications
myLocation
myMusic
myWallet
myMovies