# KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2018 onwards)

## DEPARTMENT OF COMPUTER SCIENCE, CA & IT

**SUBJECT : WIRELESS AND MOBILE COMPUTING**
**SEMESTER : I**
**SUBJECT CODE : 19CSP105A CLASS : I M.Sc.CS**

### COURSE OBJECTIVE:

This course will follow an emerging field of mobile computing applications architecture Mobility support in cellular telephone networks Personal Communications Systems/Personal Communications Networks Wireless local area networks Direct Broadcast Satellite; Low Earth Orbiting Satellites.

### COURSE OUTCOME:

- Identify the use of mobile wireless technologies
- Know the types of mobile wireless technologies that are currently being used
- Knows how does mobile wireless technologies access to network resources.

### UNIT-I

**Mobile computing applications and Platforms** - Introduction – Strengths and Weakness of Wireless – Applications – Platforms to support Mobile Computing Applications –Wireless Networks – Wireless Architecture Security and Management – Wireless Business

### UNIT-II

**Mobile Computing Applications** - Key Characteristics of Mobile Applications – Messaging for users – Mobile Portals – Special Applications – Mobile agent applications

### UNIT-III

**Wireless Internet Mobile IP and Wireless Web** - Internet and Web – How it works – Mobile IP – WWW for wireless – Mobile Web Services - **Mobile Computing Platforms** - Introduction – Wireless Middleware – Wireless Gateways and Mobile Application Servers – WAP – I-MODE Wireless JAVA MMIT and BREW – Voice communication

### UNIT-IV

**Wireless LANs** - IEEE 802.11 – MANET – HiperLAN2 - **Wireless Personal Area Networks** - IEEE 802.15 – Home Networks – Blue tooth LANs – Sensor Networks - **Cellular Networks** - Principles – First Generation(1G) Cellular – Paging networks – Second Generation(2G) Cellular – Data over Cellular Networks – Third Generation Cellular (3G) Networks – Beyond 3G

**UNIT-V**

**WML:** Formatting Output – Variables – Input Operations – WML Script – WML Libraries.

## SUGGESTED READINGS

1. Amjad Umar. (2004). Mobile Computing and Wireless Communication – Applications Networks Platforms Architecture and Security New York: NGE Solutions INC.
   (Page Nos: 1.1- 1.52 2.3 – 2.51 3.2 – 3.37 4.3-4.51 6.16-6.36 7.3-7.33 8.4-8.39)
2. Kris Jamsa. (2001). WML & WML Script. New Delhi: Tata McGraw Hill Publishing.
   (Page Nos: 61-198 225-336)
3. Ashok, K.Talukder,& Roopa, R. Yavagal. (2015). Mobile Computing New Delhi: Tata Mc-Graw Hill Publishing Company Pvt Ltd.
4. Jack, M. Holtzman, & David, J. Goodman. (2015). Wireless and Mobile Communications. Kluwer Academic Publishers.
5. Mischa Schwartz. (2015). Mobile Wireless Communications. Cambridge University Press.

## WEB SITES

1. http://www.networkcomputing.com/netdesign/wireless1.html
2. http://www.homeandlearn.co.uk/bc/beginnerscomputing.html
3. http://compnetworking.about.com/
4. http://www.compinfo.co.uk/computer_books.htm#tele

# KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)

**DEPARTMENT OF COMPUTER SCIENCE, CA & IT**

**SUBJECT : WIRELESS AND MOBILE COMPUTING**

**SEMESTER : I**

**SUBJECT CODE: 19CSP105A CLASS : I M.Sc.CS**

## LECTURE PLAN
## DEPARTMENT OF COMPUTER SCIENCE

| S.No | Lecture Duration Hour | Topics to be Covered | Support Material/Page Nos |
|---|---|---|---|
| | | **UNIT-I** | |
| 1 | 1 | **Mobile computing applications and Platforms** | T.Pg: 1-5 |
| 2 | 1 | Introduction | T.Pg: 1-5 |
| 3 | 1 | Strength and Weakness of Wireless,Applications | T.Pg: 1-5 |
| 4 | 1 | Platform to support Mobile Computing Applicatioms | T.Pg: 1- 17 |
| 5 | 1 | Wireless Networks | T.Pg: 1-27 |
| 6 | 1 | IEEE 802.11 and Bluetooth | T.Pg: 1- 31 |
| 7 | 1 | WMANs | T.Pg: 1- 31 |
| 8 | 1 | Wireless wide Area Networks | T.Pg: 1 - 36 |
| 9 | 1 | Wireless Architecture, Security and Management | T.Pg: 1 - 36 |
| 10 | 1 | Wireless Business, Wireless Internet Service Providers | T.Pg: 1 - 45 |
| 11 | 1 | Recapitulation and Discussion of Important Questions | |
| | **Total No Of Hours Planned For Unit 1=11** | | |
| | | **UNIT-II** | |
| 1 | 1 | **Mobile Computing Applications** | T.Pg: 2-3 |
| 2 | 1 | Key characteristics of Mobile Applications | T.Pg: 2-5 |

| | | | |
|---|---|---|---|
| 3 | 1 | Mobility of users | T.Pg: 2-7 |
| 4 | 1 | Target Sources, Networks | T.Pg: 2-8 |
| 5 | 1 | High Level Architecture of Mobile computing Applications | T.Pg: 2-8 |
| 6 | 1 | Message for users, | T.Pg: 2-9 |
| 7 | 1 | SMS,MMS, Applications | T.Pg: 2-9 |
| 8 | 1 | **MobilePortals, Special Applications** | T.Pg: 2 - 21 |
| 9 | 1 | Mobile Agent Applications | T.Pg: 2 - 41 |
| 10 | 1 | Recapitulation and Discussion of Important Questions | |
| | **Total No Of Hours Planned For Unit II=10** | | |
| | | **UNIT-III** | |
| 1 | 1 | **Wireless Internet** | T.Pg: 3 -2 |
| 2 | 1 | **Mobile IP and Wireless Web** | T.Pg: 3 -2 |
| 3 | 1 | Internet and Web, How it works - Mobile IP | T2.Pg: 3-5 |
| 4 | 1 | www for wireless | T2.Pg: 3 -8 |
| 5 | 1 | Mobile web Services | T2.Pg: 3 -8 |
| 6 | 1 | Mobile Computing Platforms - Introductions | T2.Pg: 3 - 14 |
| 7 | 1 | Wireless Middleware, Wireless Gateways | T2.Pg: 4- 13 |
| 8 | 1 | Mobile Application Servers - WAP - I - MODE | T2.Pg: 4 - 25 |
| 9 | 1 | Wireless Java, MMIT, BREW, voice Communication | T2.Pg: 4 - 46 |
| 10 | 1 | Recapitulation and Discussion of Important Questions | |
| | **Total No Of Hours Planned For Unit III=10** | | |
| | | **UNIT-IV** | |
| 1 | 1 | Wireless LANs - IEEE 802.11 | T2.Pg: 6 - 16 |
| 2 | 1 | MANET - HiperLAN2 | T2.Pg: 6-29 |
| 3 | 1 | Wireless Personal Area Networks | T2.Pg: 7 - 1 |
| 4 | 1 | IEEE 802.15,Bluetooth LANs | T2.Pg: 7- 15 |
| 5 | 1 | Sensor Networks | T2.Pg: 7 - 31 |

| | | | |
|---|---|---|---|
| 6 | 1 | Cellular Networks - Principles - First Generations, | T1.Pg: 8 - 20 |
| 7 | 1 | Paging, Second Generations(2G) cellular,Data Over Cellular Networks | T1.Pg: 8 - 20 |
| 8 | 1 | Third Generation cellular (3G), Beyond 3 G | T1.Pg: 21 - 30 |
| 9 | 1 | Recapitulation and Discussion of Important Questions | |
| | **Total No Of Hours Planned For Unit IV=09** | | |
| | | **UNIT-V** | |
| 1 | 1 | WML Formatting Output | T2.Pg: 61 |
| 2 | 1 | Variables | T2.Pg: 86 |
| 3 | 1 | Input Operations | T2.Pg: 123 |
| 4 | 1 | WML Script | T2.Pg: 225 |
| 5 | 1 | Libraries | T2.Pg: 256 |
| 6 | 1 | Recapitulation and Discussion of important Questions | |
| 7 | 1 | Discussion of Previous ESE Question Papers. | |
| 8 | 1 | Discussion of Previous ESE Question Papers. | |
| | **Total no of Hours Planned for unit V=8** | | |
| Total Planned Hours | | **48** | |

**SUGGESTED READINGS:**

1. Amjad Umar. (2004). Mobile Computing and Wireless Communication – Applications Networks Platforms Architecture and Security New York: NGE Solutions INC.
   (Page Nos: 1.1- 1.52 2.3 – 2.51 3.2 – 3.37 4.3-4.51 6.16-6.36 7.3-7.33 8.4-8.39)
2. Kris Jamsa. (2001). WML & WML Script. New Delhi: Tata McGraw Hill Publishing.
   (Page Nos: 61-198 225-336)
3. Ashok, K.Talukder,& Roopa, R. Yavagal. (2015). Mobile Computing New Delhi: Tata Mc-Graw Hill Publishing Company Pvt Ltd.
4. Jack, M. Holtzman, & David, J. Goodman. (2015). Wireless and Mobile Communications. Kluwer Academic Publishers.
5. Mischa Schwartz. (2015). Mobile Wireless Communications. Cambridge University Press.

**WEB SITES**

1. http://www.networkcomputing.com/netdesign/wireless1.html
2. http://www.homeandlearn.co.uk/bc/beginnerscomputing.html
3. http://compnetworking.about.com/
4. http://www.compinfo.co.uk/computer_books.htm#tele

# UNIT I

## SYLLABUS

**Mobile computing applications and Platforms** - Introduction – Strengths and Weakness of Wireless – Applications – Platforms to support Mobile Computing Applications –Wireless Networks – Wireless Architecture Security and Management – Wireless Business

### Mobile computing applications and Platforms

### 1.1 Introduction

Guglielmo Marconi invented the wireless telegraph in 1896. By encoding alphanumeric characters in analog signals, he sent telegraphic signals across the Atlantic Ocean. This led to a great many developments in wireless communication networks that support radio, television, mobile telephone, and satellite systems that have changed our lives. The wireless networks themselves have improved tremendously with notable advances in cellular networks, satellite communications, and wireless local area networks. More recently, many mobile computing applications (computing applications that run partially or completely on mobile devices) have emerged that fully exploit the capabilities of wireless networks and mobile devices. The end result is numerous developments with far-reaching impact on business, education, entertainment, and daily lifestyles. Some of the examples were highlighted in the opening vignette, "Wireless in Action – A Few Snippets."

Mobile computing and wireless communications have created several opportunities because of the appeal of wireless communications – typified by the overused slogan of "communications anytime and anywhere." However, these developments have also raised several technical and business issues and have introduced a tremendous amount of jargon and new terms (see Figure 1-1). The purpose of this unit book is to explain the technical as well as business aspects of the field that span applications, networks, platforms, architectures, security, and management issues.

## 1.2 Strengths and Weaknesses of Wireless

### 1.2.1 Strengths and Drivers

Mobile computing and wireless communication networks are playing an increasingly important role in our professional and personal lives. For example, large numbers of subscribers to mobile telephones (more than a billion in 2004) use mobile devices on a daily basis for personal and business communications. In addition, Wireless Ethernet (also known as Wi-Fi, abbreviation of Wireless Fidelity) LANs are being rapidly deployed in offices, homes, shopping malls, "hotspots," and apartment buildings. The result is a very large number of business, government, military, educational, and social applications.

The strengths of wireless systems that are driving their growth are:

**Social and cultural factors**. Wireless systems conform to our inherently mobile lifestyles. In our personal and business lives, our employees, partners, customers, relatives and friends are always moving around. Wireless systems fit well in this increasingly mobile environment with the need for information/transactions anytime and anywhere.

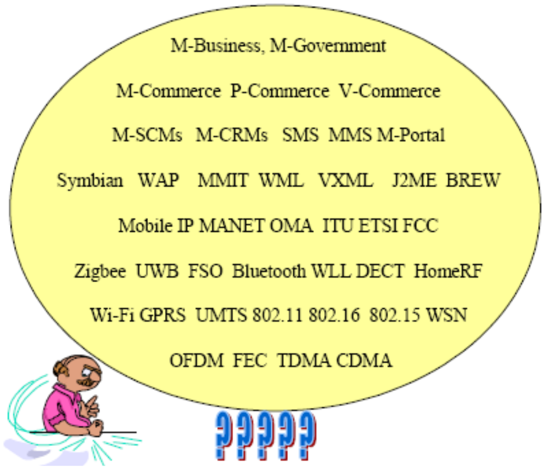

M-Business, M-Government
M-Commerce P-Commerce V-Commerce
M-SCMs M-CRMs SMS MMS M-Portal
Symbian WAP MMIT WML VXML J2ME BREW
Mobile IP MANET OMA ITU ETSI FCC
Zigbee UWB FSO Bluetooth WLL DECT HomeRF
Wi-Fi GPRS UMTS 802.11 802.16 802.15 WSN
OFDM FEC TDMA CDMA
?????

**Figure 1-1: The Mobile Computing and Wireless Jungle**

**Advances in wireless networks**. A particular appeal of wireless systems, in addition to their flexibility, is the steady increase in wireless data rates. Higher data rates are achievable with broadband wireless technology for applications such as graphics, video, and audio. Broadband wireless networks give higher data rates that compete with wired networks, plus they enjoy convenience and reduced cost. For example, 802.11g wireless LANs yield data rates in the range of 50 Mbps (million bits per second) that compete with similar wired data rates. But broadband wireless services can be deployed faster than wired services with no cost of cable plants. In addition, service is mobile, and can be deployed almost anywhere.

**Niche applications**. In some cases, wireless is the *only* option. For example, wired communications over very long distances (between the US and Australia, for example) are virtually impossible, and wireless is the only choice for space explorations. In addition, many law enforcement and battlefield applications can only work with wireless communications. For example, it is difficult to lay cables in a battlefield, or to carry a wired device when chasing a criminal.

**Special situations**. Wireless communications make more sense in several situations. For example, satellite communication is a good choice to connect far-flung and hard-to-reach areas. In addition, it may be difficult to lay cables in hostile environments. In the war-torn country of Angola, for example, it was hazardous for the workers to lay cables along roads between major cities; so wireless links were used instead. As another example, consider the following quote:

Telkom (South Africa) also prefers (wireless) technology in high-theft areas such as the corridor between Soweto and the Central Business District of Pretoria. In this area, copper cables are stolen before Telkom has time to turn on the lines. (Source: N. Baker, “Telkom South Africa: Case Study in WLL Deployment,” *Pyramid Research Report*, www.itu.int/ITU-D/fg7/case_library/ documents/pyr001.doc)

**Wireless for older buildings**. In many cases, wireless is chosen because the buildings are too old for installing cables. The University of Texas at El Paso, for example, deployed wireless networks at several campus locations because it was difficult to wire historical buildings and remote locations.

**Developments in mobile devices.** The new breed of wireless handsets have many attractive features such as digital cameras, and pictures. The availability of new mobile devices such as powerful laptop computers, PDAs, and cellular telephones with Internet and wireless data access capabilities is also driving the growth.

**Increased revenue and productivity possibilities**. The revenue opportunities created via location-based services and m-commerce have lured several companies and investors into this area. In addition, the productivity improvements to be gained via wireless extensions to enterprise applications and processes are tremendous. For example, mobile customer relationship management systems can capture customer information in real time and allow marketing reps to be more productive.

**Industrial and regulatory factors.** The convergence of telecommunications and software industries coincides with the adoption of wireless standards such as WAP and Bluetooth, along with the cultural and regulatory drivers in various countries.

### 1.2.2 Weaknesses and Issues

Wireless is convenient and less expensive but some business, political and technical difficulties inhibit wireless technologies. A major limitation is security of wireless systems because wireless communications are technically easier to eavesdrop and intrude. There are also some additional limitations. These include lack of industry-wide standards, data rate limitations as compared to wired networks (despite progress), and device limitations. For example, small LCDs on mobile telephones can only display a few lines of text, and browsers of most mobile wireless devices use specialized languages such as wireless markup language (WML) instead of HTML, making application development harder. These weaknesses can be discussed in terms of social, business, and technology issues.

#### 1.2.2.1 Social Issues

Wireless systems, despite their popularity, have raised some social issues. Privacy and security are among the top. Consider, for example, the privacy issue raised by location-based services (LBSs). Wireless networks have to keep track of the user location to direct the messages to the users as they move around. For example, cellular networks keep a Visitor

- Location Register (VLR) – a database – that records the location of a user as she moves from one cell to another. Suppose you take a train from Philadelphia to New York and turn on your cellular phone when you get on the train. Then the VLR will indicate that now you are in Philadelphia. As the train travels through "scenic" New Jersey, you will change several cells along the way (each cell is between 10 to 15 miles) and the VLR will be updated accordingly. Thus the VLR log will show when you were in Philadelphia and what path you took on your way to New York. This information traces your movement and could be considered private, but the cellular providers can sell or give this information to others – a potential privacy issue. The general concern about wireless security is that wireless networks are easier to tap into. Within this broad area, users are concerned with several privacy and security issues. For example, the call setup information that includes the user ID and other information should be protected, and the speech and data transmitted during a wireless session should be kept private and confidential. Some possible health issues have been raised due to the increased use of cellular phones and other wireless equipment. In particular, some media attention has focused on a possible link between cellular (cell) phone use and brain cancer, originally because of a lawsuit that alleged such a link. Due to the increased number of accidents caused by drivers who were talking on their cellular phones, use of cellular phones while driving has been prohibited in many states.

### 1.2.2.2 Business Issues

From a business point of view, the major hurdle is a good business case for m-business. There have to be compelling business reasons for adopting mobile communications at the enterprise level. The two important questions [Kalakotta 2002] are:

What can the customer do that could not be done before?

What can a business do that it could not do before?

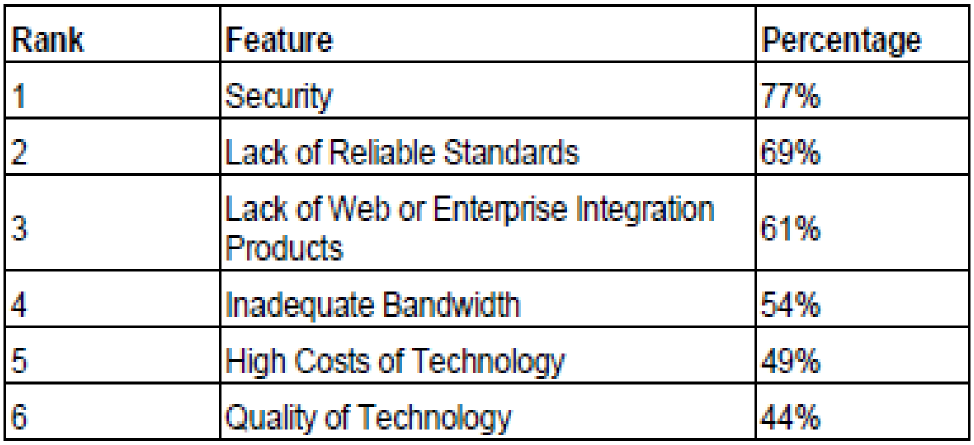
These two questions go to the heart of the matter. Of course, other questions need to be asked for developing a good business case: can a business make money by using this model; who are the customers and how will they benefit from this product or service; what exactly is the problem that is being solved; and can the end-users adopt and use this service? Variants of these questions need to be asked for new initiatives.

### 1.2.2.3 Technology Issues

Wireless systems, although improving steadily, encounter several technical barriers that deter the adoption of wireless technologies. For example, lack of security solutions at the enterprise level is a major concern. In addition, there are diverse standards for mobile computing applications, mobile computing platforms, and wireless networks that hinder adoption. The multitude of mobile devices with different form factors and capabilities, and slow and errorprone networks also do not help the cause of rapid adoption. In particular, it is difficult for wireless networks to compete with the data rates of fiber optic networks, especially if two sites can be connected easily with a fiber cable.

Different surveys at different times have stated the aforementioned reasons as the main concerns. A well-known survey was conducted by Information Week in December 2000. This survey, shown in Table 1-2, was responded to by 101 IT and business managers. Even though these concerns exist, it is possible to design wireless solutions that provide high security and provide an integrated and seamless experience to the user despite the heterogeneous networks and devices.

**Table 1-2: Wireless Internet IT Concerns (Source: Internet Week, December 2000).**



| Rank | Feature | Percentage |
|---|---|---|
| 1 | Security | 77% |
| 2 | Lack of Reliable Standards | 69% |
| 3 | Lack of Web or Enterprise Integration Products | 61% |
| 4 | Inadequate Bandwidth | 54% |
| 5 | High Costs of Technology | 49% |
| 6 | Quality of Technology | 44% |

**Mobile Computing Applications:** Supporting m-Business and m-Government Computing Applications: Supporting m-Business and Mobile computing applications support m-business, m-government, and mobile life initiatives. These applications have profound impact on the way corporations conduct their business and the way government agencies deal with the public by exploiting mobility. Specifically, these applications enable the C2B, B2B, B2E, C2G, B2G, G2G, and G2E operations between customers, business units, government agencies, and employees (see Figure 1-1.2).

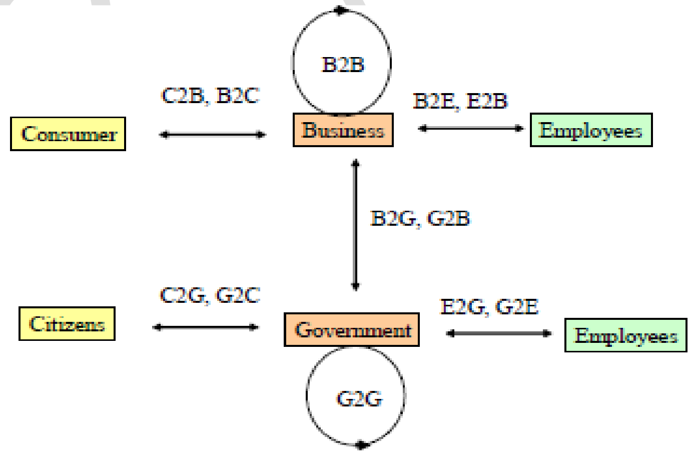


**Figure 1-1.2: Interactions Between Consumers, Business Units, Government Agencies, Citizens, and Employees**

A few observations are important before proceeding. First, most mobile computing applications are not fundamentally new applications. Instead, mobile device access over wireless networks is another aspect (dimension) of most existing arrays of applications. In fact, mobile access is being added to existing applications in a manner similar to the addition of Web access in the 1990s. Second, mobile access is not the only new feature of mobile computing applications – they also may include *positional* features that exploit location of the users, voice capabilities to support voice applications, and television features for interfacing with TV sets. These features, called MPTV (Mobile, Positional, Television, Voice) are shown in the sidebar "MPTV Applications". Finally, there are some core mobile computing applications that are being used, with minor and necessary modifications, for m-business and m-government initiatives. Examples of these applications are:

- Wireless messaging services
- Wireless Websites and mobile portals
- Mobile commerce and its variants
- Mobile customer relationship management systems (m-CRM)
- Mobile supply chain management systems (m-SCM)
- Specialized applications involving mobile agents and sensor networks

Table 1-3 shows how these core applications support the m-business, m-government and mobile life initiatives. For this reason, we will not discuss separate mobile computing applications for m-business and m-government; instead we will briefly review these applications here and briefly discuss how variants of these applications are being used in different sectors of our professional and personal lives. Chapter 2 will provide a more detailed discussion of these applications.

### 1.2.3 Wireless Messaging

Wireless messaging is an interesting and important development in wireless applications. Access to important information and communications is critical for millions of people.

Mobile users spend a significant amount of time away from their desk and can be frustrated by their inability to stay connected to the information that drives their day. In order to allow remote access to email and corporate data, mobile professionals and IT departments have been forced to live with an imposing range of technical issues, workflow interruptions and significant costs. Common complaints include: security concerns, incompatible systems, constant dialing-in, bulky equipment, missed messages and overloaded inboxes. Commonly known as "always-on email," these services are touted as the long awaited killer applications for cellular networks. Examples of these services are

- Short message services (SMS)
- Multimedia message services (MMS)
- Blackberry from Research in Motion (RIM)

These applications are used widely in m-business, m-government, and mobile life situations.

### 1.2.4 Mobile Commerce and its Variants

m-Commerce describes the phenomenon of using wireless mobile devices such as digital phones and PDAs to search the Internet, access data and information, and conduct purchasing or business transactions. m- ommerce is fueled by the extreme popularity of mobile devices such as laptop computers, cellular phones, PDAs (personal digital assistants), and palm pilots. However, the vast majority of devices and usage continue to depend on laptops and PCs, which will remain the de facto standard of devices used to access enterprise data and applications. Although the mobile PDA and telephone device markets are growing rapidly, the growth in the North American market is slower than the European and Japanese markets. However, availability of wireless platforms will play a key role in this area.

One of the main value propositions of m-commerce is its ability to personalize applications for individual users. Providers that wish to offer the best m-commerce services need information such as the user's name, address, location, and billing details (the number of a credit card or a bank account, for example). In addition, because the size of the screen affects the kind of information that can be viewed, the type of device used to connect to the service is also specified.

**Voice commerce (v-commerce)** is gaining importance to support users who want to use telephones and other voice-driven devices for conducting ecommerce. For example, while driving and walking, it is easier to use a telephone than a computer. Technologies and standards such as Voice over IP (VOIP) and Voice markup Language (VML) will play a key role in v-commerce.

**Positional commerce *(p-commerce)*** is becoming popular to provide support to customers based on their geographic position (e.g., to give you information about deals in the Boston area when you are in Boston). The systems use a GPS (Geographical Positional System) to locate the position of the customers. In addition to GPS, wireless access is at the core of mobility support – thus developments such as the Wireless Application Protocol (WAP) and Wireless Markup Language (WML) are playing a key role in this area. In addition, mobile agents are being employed widely to support p-commerce.

### 1.3 Mobile Enterprise Business Applications (M-Portals, M-CRMs, MSCMs)

Many mobile computing applications such as mobile portals, mobile customer relationship management systems (m-CRM), and mobile supply chain management systems (m-SCM) represent a mobile enablement of enterprise business applications. These *mobile* enterprise business applications (MEBAs) add the mobility capabilities to the core enterprise applications (ERPs, SCMs, CRMs, etc.) for availability to employees, partners, and customers who could be roaming around the globe. This idea has raised some issue – security and privacy are the main ones -- but MEBAs are becoming reality very quickly. Use of mobile devices such as laptop computers, personal digital assistants (PDAs), and digital telephones with Internet and wireless data access capabilities is widespread. The ability to support these highly mobile devices as part of an extended enterprise application strategy is critical. The mobile e-business applications enable mobile customers to conduct transactions with their financial services, telecommunications, or product suppliers of choice. An interesting issue is content aggregators: businesses that design and operate portals (which provide information in a category) or search facilities to help users find their way around the Internet. This function is particularly important for mobile users because mobile telephones have small screens and limited input mechanisms – notably, no mouse and a non-QWERTY (i.e., not a computer terminal) keypad. Users need mobile portals that simplify the search, avoid displaying too much information, and require minimum input. MEBAs create many opportunities such as business and revenue growth, support for new types of customers, and conformance to different social models of how and where business is conducted. But MEBAs also introduce several risks. Security and unauthorized access is a natural issue. In addition, highly mobile organizations need to manage the scores of laptops, as well as the data held on mobile devices.

In particular, these organizations need to handle data synchronization, file distribution, software distribution, and systems management tools needed for mobile applications. This problem will only grow as more and new types of devices become part of the mobile enterprise. Some companies such as Synchrologic, Inc., provide tools to manage the synchronization, distribution, and control of data to mobile users on a variety of devices. MEBAs naturally support the m-business initiative but they can be used for m-government and mobile life undertakings also. For example, mobile portals can be used by government agencies for C2G or B2G operations where agencies provide a portal for the citizens. For example, the IRS site for small-to-medium sized businesses is beginning to look like an mportal. m-Portals, for example, can be used for health as well as entertainment purposes; Web MD is an example.

**1.3.1 Specialized Applications with Mobile Agents and Sensor**

Networks Several specialized mobile applications for specialized purposes are also being developed. Let us look at mobile agents and wireless sensor networks as examples.

An ***agent*** is a software entity (i.e., a program) that has some degree of autonomy. It carries out operations on behalf of a user or another program, and in this process, represents or has knowledge of the user's goals and wishes. In this sense, a software agent is similar to a reallife agent such as a life insurance agent, a car insurance agent, a travel agent, a real estate agent, and the like. All agents, software or human, carry out a set of operations on behalf of a user (customer) – they do so with some degree of autonomy to satisfy its user's goal. Software agents, like real-life agents, can be:

- Intelligent or dumb
- Static or mobile

***Mobile agents*** are programs capable of being transferred to remote hosts in order to carry out different tasks on behalf of their users. Mobile (transportable) agents have the ability to travel through the network. A mobile agent can halt its execution, move to another host on the network while maintaining its state, and resume execution on the destination host. Mobile software agents are also similar to mobile real-life agents who travel around on your behalf instead of sitting around and making phone calls or sending email. I can, for example, ask my nephew to buy a lawn mower for me by driving around in the neighborhood instead of making phone calls and getting on websites.

Another possible area of mobile applications is ***wireless sensor networks (WSNs)*** and ***nanotechnologies***. The extremely small sensors, or nano-computers, can be "sprayed" in a particular area to gather information. For example, many sensors are installed or sprayed in an area to detect vehicle movements, collect temperature fluctuations, or gather a variety of other useful information. But these sensors are not very useful by themselves unless they form networks, called wireless sensor networks (WSNs), which carry information to control/dissemination points. In general, these devices quickly form networks and send information to remote sites. Naturally, these computers are not wired – they form Mobile Adhoc Networks (MANETs) that are used in many military and civilian applications. We will discuss WSNs in later chapters (Chapter 7 and Chapter 10). Many interesting articles on WSNs can also be found in the June 2004 issue of *Communications of the ACM*.

### 1.3.2 Mobile Computing Application Development and Support Issues

Applications for mobile users face many unique challenges because wireless networks pose unique problems that more commonly available fixed networks do not have.

Wireless networks, although improving dramatically with time, are typically slower, get congested frequently, and are more error-prone and susceptible to outages than their wired counterparts. Thus mobile computing application designers should have some knowledge of the underlying communication network. For example, database queries over wireless networks should not attempt to send thousands of rows because the network may not be available that long. Besides wireless network weaknesses, the limitations of mobile devices also need to be considered. There is a potpourri of new mobile devices, such as cell phones, pagers, and personal digital assistants (PDAs). Developing applications for these devices is challenging because they have different form factors (e.g., varying numbers of display lines), different browsers and markup languages (HTML, WML, and cHTML3), and different device capabilities (some can display images, some cannot). Special platforms, called ***mobile computing platforms***, are needed to provide the unique services needed by mobile computing applications. These platforms, discussed extensively in Chapter 4, enable the operation and, in many cases, development and deployment, of mobile computing applications. Figure 1-5, a refinement of the framework shown in Figure 1-2, depicts three type of services provided by these platforms:

**Local platform services** that support the applications on the individual mobile devices. These services consist of operating systems (e.g., Symbian OS) needed to run the mobile devices, and also include local system software services such as database managers, transaction managers, and utilities for mobile devices. These services are designed specifically to handle the unique features of the devices.

**Network transport services** that are responsible for shuffling the messages over, in this case, wireless networks. These services, mostly handled by the Internet technologies (TCP/IP, in particular), operate on top of physical wireless and wired networks to route the messages so that the mobile users can access their emails, websites, and corporate applications. Specialized protocols such as Mobile IP are needed for mobile devices.

**Middleware services** that interconnect mobile users, databases and applications with each other. For example, wireless middleware provides remote access to a corporate database from a mobile phone and may also encrypt and compress the messages for security and performance. An interesting trend at present is to package a variety of middleware services into "wireless gateways" and "mobile application servers" that can 3 WML (wireless markup language) and cHTML (compact HTML) support the current and future breed of mobile applications. Examples of such packages are WAP (Wireless Application Protocol), i-mode and J2ME (Java2 Micro Edition), and Microsoft Mobile Internet Toolkit.

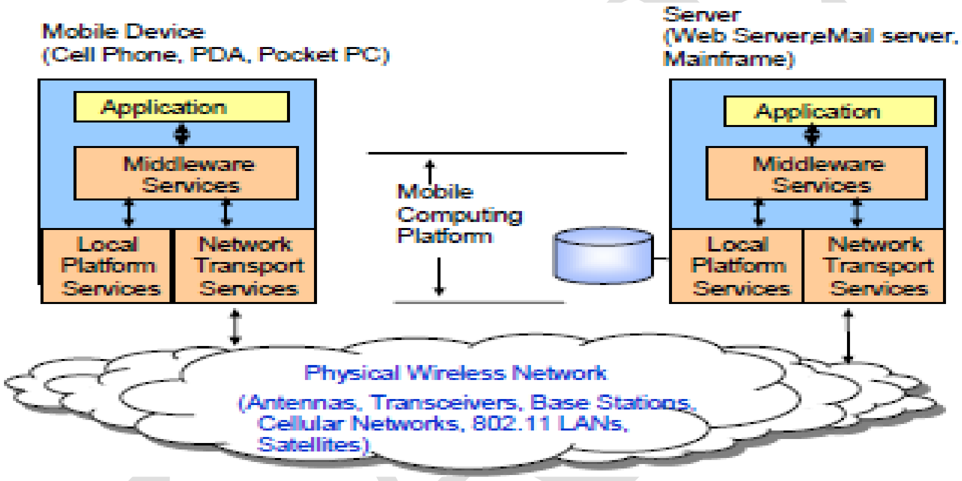

Mobile Device
(Cell Phone, PDA, Pocket PC)
Application
Middleware Services
Local Platform Services
Network Transport Services
Server
(Web Server,eMail server, Mainframe)
Application
Middleware Services
Local Platform Services
Network Transport Services
Mobile Computing Platform
Physical Wireless Network
(Antennas, Transceivers, Base Stations, Cellular Networks, 802.11 LANs, Satellites)

**Figure 1-5: Platforms for Mobile Applications**

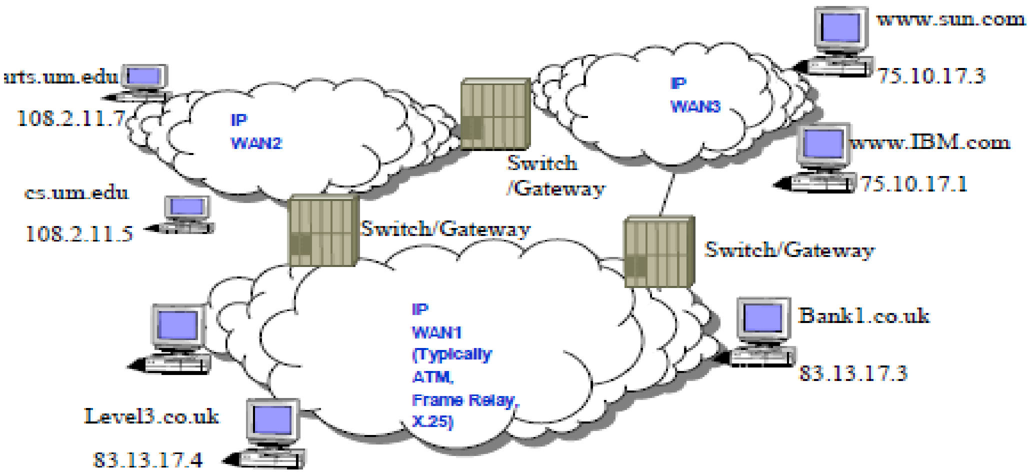
### 1.3.3 Wireless Internet, Mobile IP, and Wireless Web

Technically speaking, an Internet is a network based on the TCP/IP protocol stack. At present, the term *Internet* is used to refer to a large collection of TCP/IP networks that are tied together through network interconnectivity devices such as routers and gateways. At present, the term *Internet* is used to symbolize the following two situations:

**Public Internet**, or just "the Internet," that is not owned by any single entity – it consists of many independent TCP/IP networks that are tied together loosely.

**Private Internets**, or intranets, are the TCP/IP networks that are used by corporations for their own business – they use the same technology as the public Internet but the underlying physical network is privately owned.

**Extranets** are the TCP/IP networks that are jointly owned by corporations to conduct business. Figure 1-6 shows a conceptual and partial view of the Internet. This Internet shows three networks (a university network with two computers, a commercial company network, and a network in UK). Each computer ("host") on this network has an IP address and has been assigned a domain name as well. The Internet is very heterogeneous (i.e., different computers, different physical networks). However, to the users of this network, it provides a set of uniform TCP/IP services (TCP/IP hides many details). Once a device (mobile device or a laptop) has an IP address, then it can send messages to any other device with another IP address. Thus a user at arts.um.edu can send email to someone at bank1.co.uk and browse the IBM website



•DNS (Domain Name Services) translates cs.um.edu to 108.2.11.5
•Telnet cs.um.edu = Telnet 108.2.11.5
•FTP cs.um.edu = FTP 108.2.11.5

To support highly mobile devices, a new protocol called Mobile IP has been introduced.

Mobile IP allows mobile devices (PDAs, portable computers) to maintain Internet connectivity while moving from one Internet attachment point to another. This is done by using a concept similar to mail forwarding (the traffic is forwarded to the mobile device as it moves around).

How does wireless Web work? Web technologies reside on top of the Internet to support GUI operations. Figure 1-7 shows a conceptual view of how Web content is accessed from regular Web browsers (steps 1, 2, 3) as well as from cellular phones (steps 4, 5, 2, 3). The core building blocks of this view are:

- Web servers that are custodians of Web content and also provide access to non-Web content through Web gateways
- Web browsers that display the Web content (e.g., html pages) on PCs
- The Internet that carries the traffic between Web browsers and Web servers
- Wireless browsers that display the content on wireless handheld devices
- Wireless gateways that translate Internet protocols to wireless networks, if needed, and also convert ("render") the Web content to be displayed on handheld browsers
- Wireless networks that carry the data for handheld devices

## 1.4 Overview of Wireless Networks

### 1.4.1 A Classification of Wireless Networks

Wireless networks, as the name implies, interconnect devices without using wires – instead they use the air as the main transmission medium. Wireless networks are enjoying widespread public approval with a rapidly increasing demand. The unique features of the wireless networks are:

 The bandwidths, and consequently data rates, of communication channels are restricted by government regulations. The government policies allow only a few frequency ranges for wireless communications.

 The communication channel between senders/receivers is often impaired by noise, interference and weather fluctuations.

 The senders and receivers of information are not physically connected to a network. Thus the location of a sender/receiver is unknown prior to start of communication and can change during the conversation.

A very large body of work on wireless networks exists, with emphasis on different aspects such as radio transmission technologies, standards, protocols, systems engineering, and carriers. See, for example, the Mobile Communications Series by Artech Publishing. For our purpose, wireless networks can be broadly classified in terms of distance covered: wireless local area networks, wide area networks and metropolitan area networks. Figure 1-4.1 displays an overall classification of wireless networks in terms of distance covered, from very short range (10 meters) to very long range (thousands of miles).

**Wireless LANs** (WLANs) allow workstations in a small area (typically less than 100 meters) to communicate with each other without using physical cables. The most popular example of Wireless LANs are the IEEE 802.11 LANs that deliver between 11Mbps to 54 Mbps data rate. Another example is the Bluetooth LANs (for the data rates in the 1 Mbps range over 10 meters). Very short range LANs such as Bluetooth are also known as Wireless Personal Area Networks (WPANs)

**Wireless metropolitan area networks** (WMANs) have been used in traditional packet radio systems often used for law-enforcement or utility applications. An interesting area of growth for wireless MANs is the wireless local loop (WLL) that is quite popular with long distance telephone companies. WLLs are ***fixed wireless networks*** where the devices being connected are stationary.

**Wireless WANs** (WWANs) provide wireless support over long distances. Traditional examples of wireless WANs are paging networks and satellite systems. However, a great deal of wireless WAN activity at present revolves around the cellular networks that provide support for cellular phones and other handheld devices such as PDAs and laptops.

The wireless networks in the aforementioned categories are offering higher data rates than before. However, the wired networks are also offering higher data services. Table 1-4 summarizes the typical data rates in the wireless versus the wired world. As you can see, the wireless technology is much slower than its wired counterpart but it offers greater flexibility to the users.

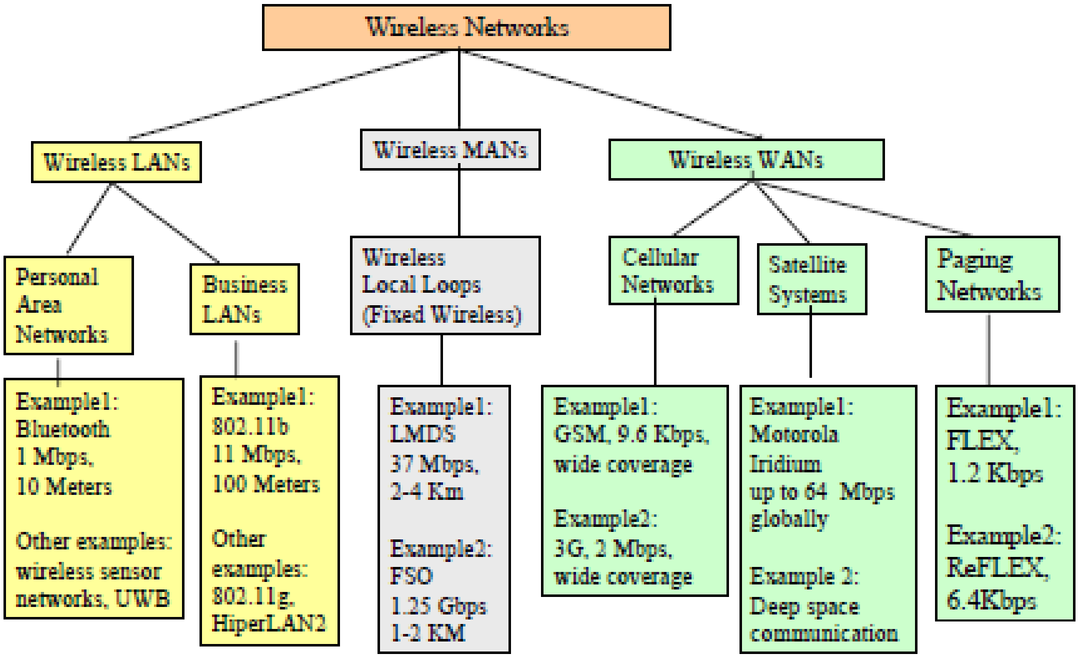

Wireless Networks
Wireless LANs
Wireless MANs
Wireless WANs
Personal Area Networks
Business LANs
Wireless Local Loops (Fixed Wireless)
Cellular Networks
Satellite Systems
Paging Networks
Example1: Bluetooth 1 Mbps, 10 Meters
Other examples: wireless sensor networks, UWB
Example1: 802.11b 11 Mbps, 100 Meters
Other examples: 802.11g, HiperLAN2
Example1: LMDS 37 Mbps, 2-4 Km
Example2: FSO 1.25 Gbps 1-2 KM
Example1: GSM, 9.6 Kbps, wide coverage
Example2: 3G, 2 Mbps, wide coverage
Example1: Motorola Iridium up to 64 Mbps globally
Example 2: Deep space communication
Example1: FLEX, 1.2 Kbps
Example2: ReFLEX, 6.4Kbps

**Figure 1-4.1: A View of Wireless Network Landscape**

### 1.4.2 Wireless LANs: IEEE802.11 and Bluetooth

Wireless LANs allow workstations in a building to communicate with each other without having to be connected to physical cables. This is a major benefit because LAN wiring can be the most expensive component of a LAN. At the time of this writing, wireless LANs have several limitations such as short distances, lack of wireless adapter cards for PCs and workstations, limited connectivity to other LANs, and relatively low speeds. However, this technology is still in its infancy. Technologies such as Bluetooth (discussed in next section) are examples. Currently available wireless LANs use one of three signal types to transmit data:

- infrared
- spread spectrum

- narrowband microwave

Infrared signals behave like ordinary light (they cannot penetrate sold objects). Thus infrared wireless LANs are limited to data transmission to line of sight. Infrared technology is simple and well proven (it is used commonly in remote controls for VCRs and TVs). In addition, infrared signals are not regulated by the Federal Communications Commission (FCC). Spread spectrum is most widely used in wireless LANs. These LANs transmit in the industrial, scientific, and medical bands designated by the FCC. These bands are not licensed but are regulated by the FCC to prevent interference. This technology was developed for military and intelligence operations (the message is “spread” over a range of frequencies to make it jamresistant).

Wireless LANs based on narrowband microwave technology use the 18.82-to-
18.87 GHz and 19.6-to-19.21 GHz frequency ranges. These frequency ranges are licensed by the FCC, which means that a vendor must be approved by the agency to use these frequency ranges. Many wireless LAN vendors consider this to be a restriction.

### 1.4.2.1 IEEE 802.11 Standard for Wireless LANs

The IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks Standards Working Group in 1990. The Working Group defined the IEEE 802.11 standard protocol for two types of networks: ad hoc and client/server networks. The 802.11 LANs are most widely used. These networks operate at 11 Mbps and 54 Mbps and can support distances between 100 feet and 500 feet. Detailed information about these LANs can be found at the Wireless LAN Association Website (www.WLANA.org). Figure 1-4.2 shows a sample environment that supports wireless Ethernet LANs so that the students can access the school server as well as the public Internet. In this configuration, several wireless access points are connected to a wired LAN that is connected to the Internet and an internal server. Each access point supports mobile computers with wireless Ethernet cards in a wireless cell that spans around 100 meters. See Chapter 6 for additional details.

### 1.4.2.2 Wireless Personal Area Networks (WPANs), Bluetooth and UWB

Wireless Personal Area Networks (WPANs) are short-range (10 meter or less) radio networks for personal, home, and other special uses. Within the WPAN family, several specifications such as Bluetooth, wireless sensor networks, and UWB (Ultra Wideband) have emerged. Bluetooth is a wireless cable replacement standard that provides a 1 Mbps data rate over 10 meters or less. It typically consists of a group of linked devices, such as a computer wirelessly connecting to a set of peripherals, known as as a “piconet.” Multiple piconets can be formed to provide wider coverage. Due to its relatively low data rates and very short distances, Bluetooth is being used in home appliances, “Bluetooth-enabled” cars, and other such applications. Figure 1-4.3 shows a simple Bluetooth configuration. Bluetooth was designed to allow low-bandwidth wireless connections to become so simple to use that they seamlessly mesh into your daily life. A simple example of a Bluetooth application is updating your cellular phone directory. The main idea is that this could happen automatically as soon as the phone is within the range (10 meters) of your desktop computer where your directory resides.

**UWB (Ultra Wideband)** is a relatively new4 technology and is stronger than the other shortrange wireless systems (such as Bluetooth) because of its simpler device designs, lower power consumption and higher data rates. Another player in the short-range radios is the **wireless sensor networks (WSNs)** that are formed between small, low-powered sensor devices mainly for monitoring and data collection purposes. Yet another player in short-range wireless, HomeRF, was primarily aimed at the needs of the small office and home office (SOHO) networks. This effort has been currently sidelined due to the popularity of other alternatives such as Bluetooth and UWB.

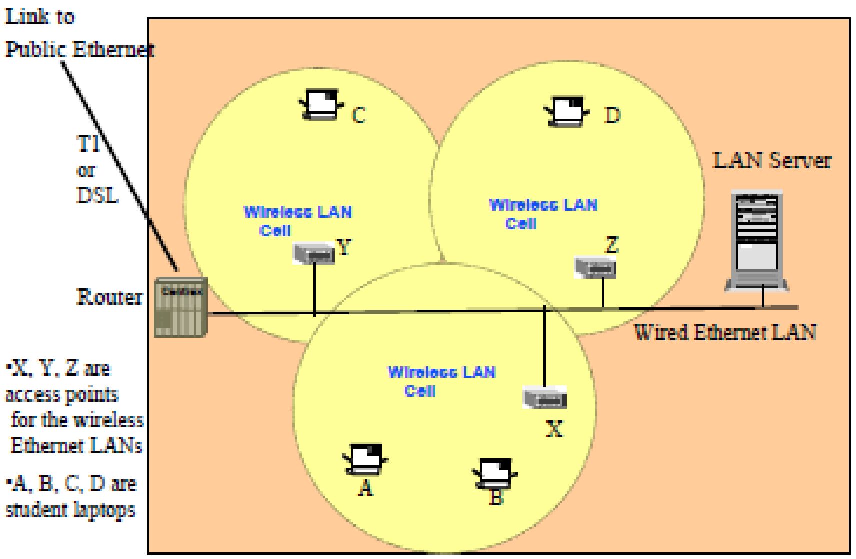


**Figure 1.4.2: A Sample Configuration with Wireless Ethernet LANs**

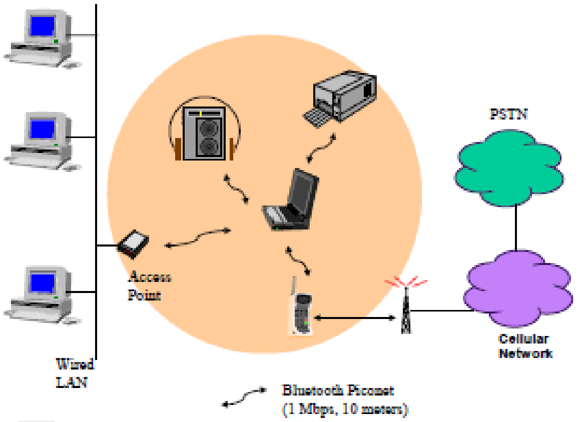


**Figure 1-4.3: A Simple Bluetooth Configuration**

### 1.5 Wireless Architectures, Security and Management

### 1.5.1 Integrated Architectures for Wireless Systems

Architectures play a vital role in wireless systems because they show how the individual systems tie together to satisfy the overall requirements. Simply stated, an architecture of a system is a structure that describes three things:

- Components of the system (what are the pieces of a system?)
- Functions performed by the components (what do they do?)
- Interfaces/interactions between the components (how do they work with each other?)

Our interest is in ***"integrated architectures"*** that consist of components that are, to some extent, *seamlessly* combined to support similar conventions or styles. An integrated architecture does not focus on one type of components, but instead combines wireless applications with the underlying IT infrastructure, including wireless network architecture.

Specifically, an integrated wireless architecture would provide seamless access to a diverse array of resources across a hybrid network of wireless LANs, cellular networks (3G, 2.5G, GSM), Bluetooth WPANs, and a variety of public shared "hotspot" LANs in hotels, restaurants, airports, plazas, gas stations or other business centers. Figure 1.5.1 suggests an integrated architectural vision that serves the needs of mobile workers and enterprises through a hybrid network architecture consisting of public shared or private wireless LANs and public-shared wireless wide area networks. The architecture presents a mixture of wireless LANs, cellular networks (3G, 2.5G, GSM), Bluetooth WPANs, and a variety of public shared "hotspot" wireless LANs in hotels, restaurants, airports, plazas, gas stations or other business centers. The growth of hotspots is an interesting development because they are filling the void as the 3G networks are being delayed. The main idea is that a wide range of individual wireless networks and fixed wireless LANs are interconnected through a mixture of wireless or wired networks to provide seamless services over the Internet. This architecture provides high-speed (IEEE 802.11b LAN at 11 Mbps or 802.11g up to 54 Mbps) access within the hotspots and business LANs and lower-speed access (56 Kbps to 384 Kbps) when outside the LANs by utilizing GSM or 2.5G GPRS cellular networks. Bluetooth technology, although not as popular as 802.11, has found a niche in the wireless personal area networks (WPANs). This vision also allows the user to perform different activities as they move from location to another. At a hotspot, for example, the user could do Web surfing and other Internet information-related work, and receive SMS messages while walking around or driving around in a car. The user can stay logged on and stay in touch, for example, even though 802.11 LAN signals fade, as the GPRS wireless WAN takes over. Thus different models of human interactions can be supported – relaxed and intense work while stationary at different sites but occasional short emails while in motion – without having to log on/log off [Dharwan 2000].

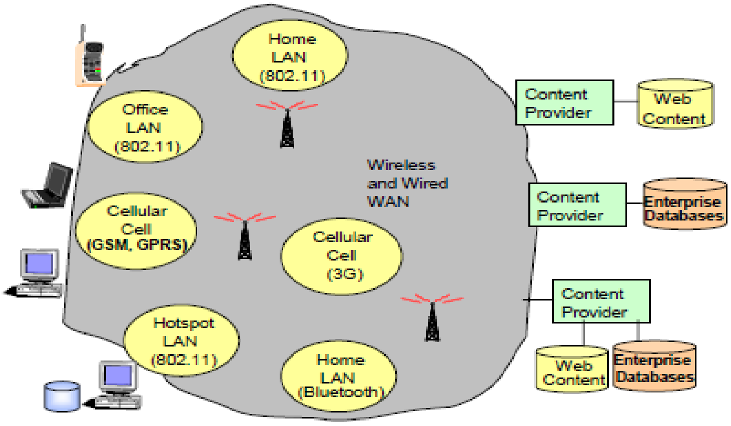


**Figure 1.5.1: A Wireless Architectural Vision**

Integrated architectures involve a continuum of services that go from low-level network interconnection technologies to business applications and processes. Specifically, integration in wireless systems requires facilities at the following levels (see Figure 1-5.2).

**Physical communication level (Layer 1 and 2)**. At the very basic level, adapter cards are needed that can detect if a user is in a different coverage area. For example, a card that can recognize GSM, GPRS, and 802.11 signals is needed in mobile devices to operate in a hybrid wireless network. In addition, network protocol converters and gateways are needed between different types of networks.

**Handoffs and roaming support between multiple networks**. Mobile IP is a major player in supporting handoffs as the mobile devices roam from one network to another and as the IP addresses change due to the roaming.

**Mobile computing platforms for integration.** At higher levels, mobile computing platforms provide the middleware services such as WAP and i-mode to shield the applications developers from the underlying network heterogeneities. Mobile application servers, such as the Oracle9iAS-wireless server, combine several middleware services into a single platform.

**Application and user interfaces.** At the application level, consistent user interfaces are needed for seamless operations. Microbrowsers and specialized markup languages such as WML (wireless markup language) support these facilities and also provide access to back-end systems.

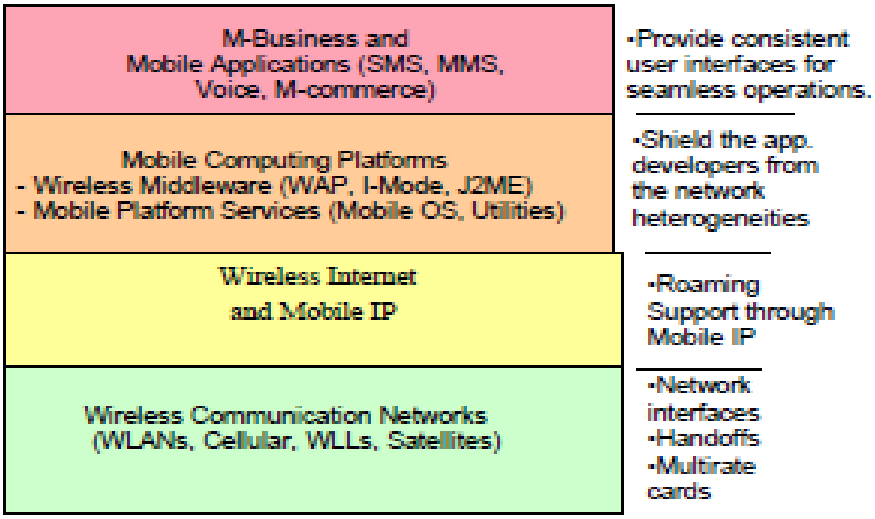

M-Business and
Mobile Applications (SMS, MMS, Voice, M-commerce)
•Provide consistent user interfaces for seamless operations.
Mobile Computing Platforms
- Wireless Middleware (WAP, I-Mode, J2ME)
- Mobile Platform Services (Mobile OS, Utilities)
•Shield the app. developers from the network heterogeneities
Wireless Internet and Mobile IP
•Roaming Support through Mobile IP
Wireless Communication Networks (WLANs, Cellular, WLLs, Satellites)
•Network interfaces
•Handoffs
•Multirate cards

**Figure 1-5.2: A Framework for Integration**

By using many of these different technologies, mobile users can move from wired to wireless networks in a seamless manner. The mobile devices need a network adapter card that will tune to a wireless LAN or WAN as the users roam from the coverage area of LANs or WANs, respectively. For example, the mobile device will tune into a hotspot LAN when you enter the coverage area of the local LAN. The software in the mobile devices will dynamically load drivers to connect to the right type of network. The middleware and application interfaces maintain the logical connection while switching from one network to the other.

### 1.5.3 Wireless Security

The growth of wireless networks and mobile services over the last few years has been tremendous. Naturally, the security concerns are becoming more serious, concomitant with the growth of wireless. As more people access critical information, and as consumers begin to do their business and banking on devices that are connected over wireless LANs, MANs, and WANs, wireless security has moved to the forefront. In essence, wireless networks face the same type of security issues (e.g., privacy, integrity, authentication) as the wired networks. Wireless security therefore is not much different from wired security. The same security concerns exist, wired or not: authenticate whom you are talking to, secure the data as it travels from the handheld device to the destination host, and ensure that the traffic has not been altered enroute. Companies such as Amazon.com and ETrade do this in the wired world. However, wireless has some unique difficulties such as limited bandwidth, high latency and unstable connections. The main differentiating issue of wireless network security is that the information is transmitted over a common medium (the air). Thus it is easier to tap into wireless traffic. There are a number of stories about eavesdropping of wireless traffic. For example, competitors have been able to capture the emails between HP personnel by simply sitting in the office parking lot with an antenna. Something similar also happened to Sun Microsystems. In addition, information sent by a federal agency wirelessly was intercepted and then used against the agency in a future negotiation. My own students, from a wireless network class that I taught, spent a day in Manhattan and captured a disk full of plain text (unencrypted data) by simply driving around the Manhattan business district in a car with a simple antenna. wireless security and attempts to answer the following questions:

- What are the core security principles?
- What are issues specific to wrireless LANs, cellular networks, satellites, WLLs, and cordless?
- How can TCP/IP security through VPNs and IPSec be used to secure wireless communications?
- How do higher-level security such as for WAP and SET interplay with wireless network security?
- Can a comprehensive wireless security procedure be developed that considers all security levels?

The issues of security are of vital importance for mobile services and need more attention. Basically, security involves the following aspects, called PIA4:

**Privacy:** ensure confidentiality of information (i.e., no one other than the authorized people can see the information) when transmitting it over a network or storing it in a insecure place.

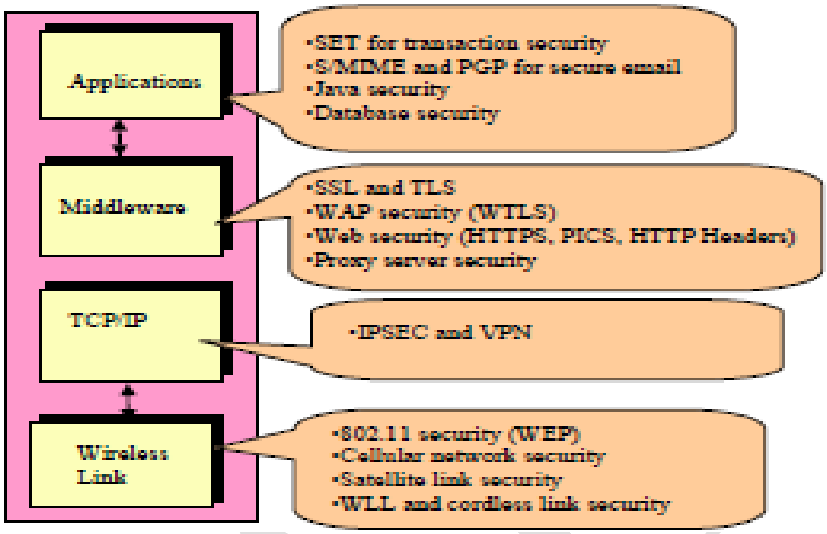
**Integrity:** avoid corruption of information (i.e., no unauthorized modification allowed).

**Authentication:** identify for certain who is communicating with you (i.e., make sure that you are who you say you are).

**Authorization (Access control):** determine what access rights that person has (i.e., can you only read given information or can you also update, delete, add information?).

**Accountability and Assurance:** ensure that you can tell who did what when, and convince yourself that the system keeps its security promises. This includes ***nonrepudiation(NR)*** – The ability to provide proof of the origin or delivery of data. NR protects the sender against a false denial by the recipient that the data has been received. It also protects the recipient against false denial by the sender that the data has been sent.

In other words, a receiver cannot say that he/she never received the data, and the sender cannot say that he/she never sent any data. You also need to administer the security system, i.e., define and enforce the security policies that are consistent across all elements of applications, middleware services, and networks. These, and other aspects of security, are supported at various levels (network, middleware, application) by using a wide range of technologies (see Figure 1-5.7). Security is needed at these different levels since security at each level fulfills different requirements. Figure 1-5.7 can serve to build a comprehensive checklist for security design. Let us briefly review the security at various levels. Wireless link security protects information transfer over radio links such as wireless LANs, cellular networks, satellites, and wireless local loops. Independent of the physical link, the network traffic can be encrypted at a higher level (TCP/IP) by using IPSec and VPNs. At the middleware level, SSL (Secure Socket Layer) is used for secure Web browser-Web server exchanges, and WTLS (Wireless Transport Layer Security) is used to secure WAP applications. A variety of security approaches exist at the application level, in which case authorization controls are used within applications to regulate access to specific data, and cryptographic infrastructures are built to strongly authenticate users and provide confidentiality. Examples of application level security is provided by database managers, Java Virtual Machines, email security packages (e.g., S-MIME), and SET (Secure Electronic Transactions). In particular, applications themselves provide access control and strong user Authentication



Security must be considered at all levels. Securing a higher layer while keeping lower layers unsecured makes the system vulnerable to intrusions from the lower layers. In general, lack of security at a certain layer might compromise the overall system even if other layers are secured. Consider, for instance, a system where the application data is secure, but is transmitted over an insecure network. In this case, the overall security of the application could be suspect. Specifically, application security protects application data (e.g., database security mechanisms allow the data to be stored on the hosts in a protected manner) and system resources (e.g., Java Security) while SSL protects data while being transferred on the network.

## 1.6 The Wireless Business – A Quick Scan

### 1.6.1 The Players in Wireless Business

Wireless is a multi-billion dollar business with a very wide range of players that provide different types of services, equipments, end-user devices, software packages, and consulting/integration support. There are many different views of the wireless business.7 On a personal note, this Act had a great impact on my own life. The Act caused the breakup of Bell Labs into Bellcore (Bell Communications Research) and AT&T Bell Labs. I worked at Bellcore for more than a dozen years and am still involved in many projects on a consulting basis.

Figure 1-5.8 shows a simplified conceptual view that uses the framework. The figure shows the main business sectors and illustrates one view of the complex and multidimensional aspects of wireless business in terms of the physical communication network, network transport and connectivity services, mobile computing platforms, and mobile computing applications. Some business sectors concentrate on higher-level services such as mobile applications, while others provide the low-level network elements. As expected, one large business may be involved in many business sectors, and vice versa. Similarly, many small businesses may provide different elements of one business sector. We will examine different scenarios later in this section.

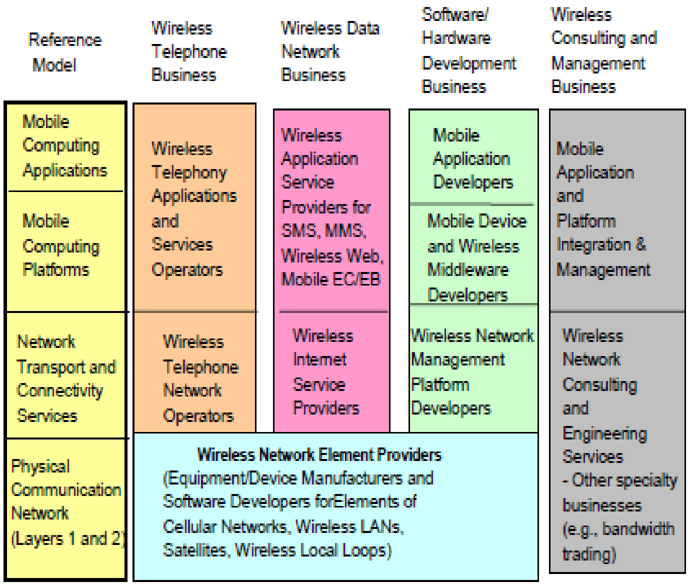

Reference Model
Wireless Telephone Business
Wireless Data Network Business
Software/ Hardware Development Business
Wireless Consulting and Management Business
Mobile Computing Applications
Mobile Computing Platforms
Network Transport and Connectivity Services
Physical Communication Network (Layers 1 and 2)
Wireless Telephony Applications and Services Operators
Wireless Telephone Network Operators
Wireless Application Service Providers for SMS, MMS, Wireless Web, Mobile EC/EB
Wireless Internet Service Providers
Mobile Application Developers
Mobile Device and Wireless Middleware Developers
Wireless Network Management Platform Developers
Mobile Application and Platform Integration & Management
Wireless Network Consulting and Engineering Services - Other specialty businesses (e.g., bandwidth trading)
Wireless Network Element Providers
(Equipment/Device Manufacturers and Software Developers forElements of Cellular Networks, Wireless LANs, Satellites, Wireless Local Loops)

**Figure 1-5.8: Conceptual View of Telecom Business**

A major business sector, Wireless Network Element Providers, builds horizontal capabilities that are needed by many vertical businesses. Businesses involved in this sector build the basic network elements of wireless networks. For example, these businesses build base stations for cellular networks, communication satellites and satellite dishes for satellite communications systems, antennas and transceivers for the wireless local loops, and access points for the wireless LANs. Other business sectors concentrate on mobile devices (e.g., cellular handset manufacturers, PDA manufacturers, etc.) and wireless middleware providers such as WAP and i-mode gateway providers. An active business sector is the application service providers (ASPs) that support mobile applications on a rental basis (see Chapter 13 for details). Several vertical business use the element providers' equipments and devices, and package them with other capabilities from other sectors to deliver services to different consumers. For example, the wireless telephone network businesses (e.g., T-Mobile) provide the telephone services over wireless, mostly cellular, networks. However, now some companies such as Vocerra systems are beginning to provide telephone services over 802.11 LANs. The wireless Internet service providers (WISPs) primarily enable wireless Web and mobile computing applications (e.g., m-commerce) over wireless networks.

A WISP is essentially an ISP that connects its subscribers to the public Internet through *wireless* connections instead of the wired DSL, cable modem, or dial-up lines. These services are commonly provided by using IP (in some cases Mobile IP) over digital cellular networks or wireless LANs. A large number of businesses develop software and hardware for the different business sectors – ranging from handsets to network monitors and mobile supply chain management systems. Due to the complexity of wireless systems, many wireless management and consulting businesses specialize in planning. organizing, staffing, engineering, re-engineering, and managing wireless initiatives. The consulting and management businesses can operate at lower layers (e.g., re-engineering of wireless networks, integration of wired with wireless networks) or at higher layers (e.g., management and integration of mobile applications and middleware services). See Chapter 13 for more details. It is important to note that that the purpose of this section is to give a broad overview of the wireless business that could help in understanding the various mobile computing and wireless initiatives. The names of the companies mentioned here are not exhaustive and may change with time in this turbulent marketplace. For an up-to-date list of the key players, it is best to visit the websites such as www.palowireless.com, www.mbusinessdaily.com, and www.mobileinfo.com.

**POSSIBLE QUESTIONS**

**UNIT I**

**PART-A (Online Examinations)**

**PART-B (5 X 6 = 30 Marks)**

**(Answer ALL the Questions)**

1. Elucidate about Strengths and Weakness of Wireless networks.
2. Enlighten on Wireless Business with example.
3. What is a mobile computing platform, what are its main components and how do these components support mobile computing applications?
4. Discuss on Wireless Security and Management.
5. Why is security such an important issue in wireless? List the main issues and approaches to deal with wireless security at various levels.
6. Discuss Mobile computing applications with example.
7. Elucidate on wireless architecture and its components?
8. What is mobile commerce and what are its main variants? Explain.
9. What is a mobile computing platform, what are its main components and how do these components support mobile computing applications?
10. Discuss in detail about wireless networks.

**PART-C (1 X 10 = 10 Marks)**

1. Compare and contrast the various types of wireless networks.
2. Elucidate the need for sensor networks with examples.
3. Elucidate in detail about generation of cellular networks.
4. List out the functions in the WML libraries with examples for usage.

5. Write in detail about WML script.

**KARPAGAM ACADEMY OF HIGHER EDUCATION**
**Coimbatore - 641021.**
**(For the candidates admitted from 2019 onwards)**

**DEPARTMENT OF COMPUTER SCIENCE,CA & IT**

## WIRELESS AND MOBILE COMPUTING - 19CSP105A

**UNIT I :(Objective Type/Multiple choice Questions each Question carries one Mark )**

**PART-A (Online Examination)**

| S.NO | QUESTIONS | OPTION 1 | OPTION 2 | OPTION 3 | OPTION 4 | KEY |
|---|---|---|---|---|---|---|
| 1 | FAA Means | **Federal Aviation Administration** | Federal Air Administration | Federal Aviation Analysis | Flexible Aviation | **Federal Aviation Administration** |
| 2 | LBS Means | Location Based Security | **Location Based Service** | Location Before Security | Location Based Secrecy | **Location Based Service** |
| 3 | WLL Means | Wired Local Loop | Wired Local Link | **Wireless Local Loop** | Wireless Local Link | **Wireless Local Loop** |
| 4 | PBS Means | Public Broad-line Service | Private Broadcasting System | Public Broadcasting Service | **Public Broadcasting System** | **Public Broadcasting System** |
| 5 | Wi-Fi Means | **Wireless Fidelity** | Wired Fidelity | Wireless Fidelities | Wireless Free | **Wireless Fidelity** |
| 6 | 802.11g standard wireless LAN supports the following any one data transfer | 100 Mbps | **50 Mbps** | 1000 Mbps | 20 Mbps | **50 Mbps** |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| 7 | VLR means | Visitor Location Record | Visitor Location Report | **Visitor Location Register** | Visitor Level Register | **Visitor Location Register** |
| 8 | NGE means | New Generation Enterprises | Next Group Enterprises | Next Generation Employees | **Next Generation Enterprises** | **Next Generation Enterprises** |
| 9 | BAM means | **Business Activity Monitoring** | Business Action Monitoring | Busy Activity Monitoring | Business Activity Method | **Business Activity Monitoring** |
| 10 | MEBA's means | Mobile E-Business Approaches | **Mobile E-Business Applications** | Mobile E-Commerce Applications | Motion E-Business Applications | **Mobile E-Business Applications** |
| 11 | C2G means | Customer-to-Government | Consumer-to-Government | **Citizen-to-Government** | Citizen-to-Governance | **Citizen-to-Government** |
| 12 | B2G means | Business-to-Governance | Business-towards-Government | Buyer-to-Government | **Business-to-Government** | **Business-to-Government** |
| 13 | B2B means | **Business-to-Business** | Business-towards-Business | Business-to-Busies | None of these | **Business-to-Business** |
| 14 | G2G means | Government-to-Governance | **Government-to-Government** | Government-towards-Government | None of these | **Government-to-Government** |
| 15 | C2B means | Consumer-to-Buyer | Citizen-to-Business | **Consumer-to-Business** | None of these | **Consumer-to-Business** |
| 16 | B2C means | Business-towards-Consumer | Business-to-Citizen | Business-to-Customer | **Business-to-Consumer** | **Business-to-Consumer** |
| 17 | B2E means | **Business-to-Employee** | Business-towards-Employee | Buyer-to-Employee | None of these | **Business-to-Employee** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 18 | E2B means | Employee-towards-Business | **Employee-to-Business** | Employee-to-Buyer | None of these | **Employee-to-Business** |
| 19 | G2C means | Government-towards-Citizen | Government-to-Consumer | **Government-to-Citizen** | None of these | **Government-to-Citizen** |
| 20 | E2G means | Employee-towards-Government | Employee-to-Governance | Employee-towards-Governance | **Employee-to-Government** | **Employee-to-Government** |
| 21 | G2E means | **Government-to-Employee** | Governance-to-Employee | Government-towards-Employee | None of these | **Government-to-Employee** |
| 22 | WSN’s means | Wired Sensor Networks | **Wireless Sensor Networks** | Wireless Sensitive Networks | None of these | **Wireless Sensor Networks** |
| 23 | MPTV means | Mobile, Positional, Telephone, Voice | Mobile, Post, Television, Voice | **Mobile, Positional, Television, Voice** | None of these | **Mobile, Positional, Television, Voice** |
| 24 | SMS means | Small Message Service | Short Method Service | Short Message Security | **Short Message Service** | **Short Message Service** |
| 25 | MMS means | **Multimedia Message Service** | Multimedia Method Service | Multimedia Message Security | None of these | **Multimedia Message Service** |
| 26 | V-Commerce means | Voice Control | **Voice Commerce** | Value Commerce | None of these | **Voice Commerce** |
| 27 | VOIP means | Value Over IP | Voice Over IR | **Voice Over IP** | None of these | **Voice Over IP** |
| 28 | VML means | Value Markup Languages | Voice Mark Languages | Voice Markup Level | **Voice Markup Languages** | **Voice Markup Languages** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 29 | WAP means | **Wireless Application Protocol** | Wired Application Protocol | Wireless Application Provider | None of these | **Wireless Application Protocol** |
| 30 | P-Commerce means | Positional Control | **Positional Commerce** | Post Commerce | None of these | **Positional Commerce** |
| 31 | Agent is a | Hardware Entity | Firmware | **Software Entity** | None of these | **Software Entity** |
| 32 | DNS means | Done Name Services | Domain Name Systems | Domain Nature Services | **Domain Name Services** | **Domain Name Services** |
| 33 | WAE means | **Wireless Application Environment** | Wireless Application Entity | Wired Application Environment | None of these | **Wireless Application Environment** |
| 34 | MMIT means | Microsoft Mobile Intranet Toolkit | **Microsoft Mobile Internet Toolkit** | Microsoft Mobile Internet Tools | None of these | **Microsoft Mobile Internet Toolkit** |
| 35 | WPAN's means | Wired Personal Area Networks | Wireless Professional Area Networks | **Wireless Personal Area Networks** | None of these | **Wireless Personal Area Networks** |
| 36 | SoHo means | **Small Office and Home Office** | Simple Option and Home Option | Simple Office and Home Office | None of these | **Small Office and Home Office** |
| 37 | LMDS means | Local Multi Distribution System | **Local Multipoint Distribution System** | Local Multipoint Distribution Service | None of these | **Local Multipoint Distribution System** |
| 38 | FSO means | Free Search Option | Free Service Optics | Free Space Option | **Free Space Optics** | **Free Space Optics** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 39 | WMAN’s means | **Wireless Metropolitan Area Networks** | Wireless Metro Area Networks | Wireless Metropolitan Area Netware | None of these | **Wireless Metropolitan Area Networks** |
| 40 | BTS means | Base State Receivers | **Base Station Receiver** | Basic Station Receiver | None of these | **Base Station Receiver** |
| 41 | GEO Satellite means | Gigabit Synchronous | Geo Synch | **Geo Synchronous** | None of these | **Geo Synchronous** |
| 42 | ASP means | Application Switch Protocols | Application Service Prototypes | Analog Service Protocols | **Application Service Protocols** | **Application Service Protocols** |
| 43 | WISP means | **Wireless Internet Service Protocols** | Wired Internet Service Protocols | Wireless Intranet Service Protocols | None of these | **Wireless Internet Service Protocols** |
| 44 | WNE means | Wireless Netware Elements | **Wireless Network Elements** | Wired Netware Elements | None of these | **Wireless Network Elements** |
| 45 | DBS means | Direct Broadcast States | . Direct Broadband Stations | **Direct Broadcast Stations** | None of these | **Direct Broadcast Stations** |
| 46 | CTI means | Connect Telephony Integration | Computer Telephony Interaction | Computer Tele Integration | **Computer Telephony Integration** | **Computer Telephony Integration** |
| 47 | FOIP means | **FAX Over IP** | FAXes Over IP | FAX Over IPs | None of these | **FAX Over IP** |
| 48 | CEM means | Consult Environment and Management | **Consulting Engineering and Management** | Consulting Engineering and Manager | None of these | **Consulting Engineering and Management** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 49 | M-CRM means | Mobile Customer Relationship Method | Mobile Citizen Recover Management | **Mobile Customer Relationship Management** | . None of these | **Mobile Customer Relationship Management** |
| 50 | GPS means | Geographical Positional Service | Group Positional System | Geographical Post System | **Geographical Positional System** | **Geographical Positional System** |
| 51 | IVR means | Interactive Voice Responses | Interaction Voice Response | **Interactive Voice Response** | None of these | **Interactive Voice Response** |
| 52 | ERP means | **Enterprise Resource Planning** | Enterprise Resource Providers | Enterprise Recover Planning | None of these | **Enterprise Resource Planning** |
| 53 | MAMs means | Mobile Asset Management Service | **Mobile Asset Management Systems** | Mobile Asset Movement Systems\ | None of these | **Mobile Asset Management Systems** |
| 54 | M-CRM means | Mobile Customer Relationship Method | Mobile Citizen Recover Management | **Mobile Customer Relationship Management** | None of these | **Mobile Customer Relationship Management** |
| 55 | GPS means | Geographical Positional Service | Group Positional System | Geographical Post System | **Geographical Positional System** | **Geographical Positional System** |
| 56 | M-SCM means | **Mobile Supply Chain Management** | Mobile Supply Chain Method | Mobile Sales Chain Management | None of these | **Mobile Supply Chain Management** |
| 57 | T-Commerce means | True Commerce | **Television Commerce** | Television Connection | None of these | **Television Commerce** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 58 | “Pushing” means | Information from mobile users | Both a and c | **Information to mobile users** | None of these | **Information to mobile users** |
| 59 | SMSC means | Short Message Secure Center | Short Method Service Center | Small Message Service Center | **Short Message Service Center** | **Short Message Service Center** |
| 60 | HLR means | **Home Location Register** | Home Locate Register | Home Location Recover | None of these | **Home Location Register** |

## UNIT-II

## SYLLABUS

**Mobile Computing Applications -** Key Characteristics of Mobile Applications – Messaging for users – Mobile Portals – Special Applications – Mobile agent applications

### 2.1 Mobile Computing Applications – Supporting m- Business and m-Government

Mobile computing applications are the key enablers of m-business. Beyond business, these applications are also supporting our daily life by providing wireless access to health services, government services, entertainment, and other social activities. These applications enable the C2B, B2B, B2E, C2G, B2G, G2G, and G2E operations between customers, business units, government agencies, and employees (see Figure 2-1). The following core mobile computing applications are being used, with minor and necessary modifications, for m-business and mgovernment initiatives:

Wireless messaging services

Wireless websites and mobile portals

Mobile e-commerce and its variants

Mobile customer relationship management systems (M-CRM)

Mobile supply chain management systems (M-SCM)

Specialized applications involving mobile agents and wireless sensor networks

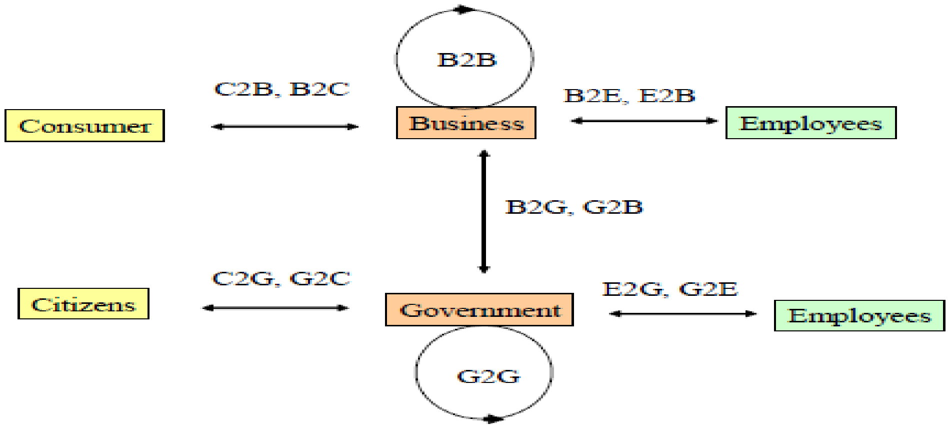


**Figure 2-1: Interactions between Consumers, Business Units, Government Agencies, Citizens, and Employees**

### 2.2 Key Characteristics of Mobile Computing Applications

### 2.2.1 Highlights of Mobile Computing Applications

Most mobile computing applications, especially in the domain of mobile e-busisness applications (MEBAs), are not fundamentally new. Instead, mobile device access over wireless networks is another capability that is being added to the current array of applications. Most suppliers of enterprise software are adding another mobility module to their current suite of enterprise applications. For example, SAP has added mobility modules to its suite of ERP (enterprise resource planning) applications. Siebel, Oracle, and PeopleSoft have followed similar approaches. In fact, most companies that are using mobile computing applications at present have extended their current corporate applications to include mobility. A good example is mobile CRM – most early adopters of M-CRM are the companies that already have a CRM in place and are now adding mobility features to support a mobile sales force. Of course, there are exceptions to this. In particular, development of wireless sensors, mobile agent applications, and some location-sensitive applications are fundamentally new applications that are unique to wireless and mobile computing. While many mobile computing applications have been developed, and more will be developed in the future, the search for "killer" applications – the applications that are phenomenally successful – continues. In reality, the killer mobile applications may vary by industry type, country, culture, and individual user. For example, mobile messaging services such as SMS are very popular in m-government, and M-SCM systems are more popular in manufacturing organizations. It is not enough to build a good application with nice features; other factors should be considered for market adoption. The market adoption of an application can be hindered by social barriers such as privacy concerns, business barriers such as revenue expectations, and technology barriers such as product maturity, usability, bandwidth, and cost. The killer applications create business value or meet unmet needs. So how are the mobile computing applications creating business value? Here are some possible ways, suggested by [Kalakotta 2004]:

**Mobile asset management**. Large companies have their assets (equipments, finished goods, raw materials, support materials, computing devices) at different locations. Mobile asset management systems (MAMs) allow the plant maintenance technicians, warehouse supervisors, and other employees to scan and capture the information about assets on-site through mobile devices. This information is then submitted electronically to the corporate systems, instead of through a paper-based system where the information is gathered manually and then entered manually into the corporate system.

**Mobile field service**. The field service technicians, when on call, use mobile devices to record the activity on-site, what was done, customer comments, etc. This log of activity is sent to corporate systems electronically. As different technicians work on the same problem, each technician can download relevant activities so far, take appropriate actions, and then log additional activities as they are performed. One of the largest users of this feature is UPS, whose parcel delivery drivers record the delivery information, customer signatures, etc. on-site .

**Mobile sales support**. Real-time support of sales force in the field through mobile devices is highly valuable because sales reps can take orders, give real-time quotes, and ensure that items are in stock and can be delivered on time before closing a deal. Due to these benefits, mobile sales support is one of the fastest growing mobile computing application.

**Mobile procurement.** The ability to acquire products quickly provides many benefits to organizations. Employees in the field can use a mobile device to search catalogs, compare prices and availability, and place orders without having to call the central office or waiting to return to the office. This application is not limited to businesses only. The physicians in Children's Hospital in Wisconsin can order new drugs quickly when they visit a patient by using a wireless-enabled laptop that they wheel around on a mobile cart during their patient visit.

The mobile computing applications that provide the aforementioned business value can be discussed in terms of the traditional C2B, B2B, and B2E applications.

**Mobile C2B/G.** Mobile enablement of customers can take many forms: specialized cell phones or pagers to increase customer loyalty; access to hotel and airline reservations and information; telematics services for emergency location and assistance; wireless access to order status information; product and service information via wireless enablement of a corporate website;

alerts and notifications on items of interest; location-based services for marketing; unified messaging for customer support.

**Mobile B/G2E**. Wireless enablement for employees basically gives employees the access to the information and transactions they need in order to perform their work-related activities. Wireless enablement can be an extension of existing enterprise applications or it can take be entirely new applications built specifically for use in a wireless or mobile scenario. These applications, if done right, can have a profound productivity improvement for employees, the sales force, the field force, and for executives within an enterprise.

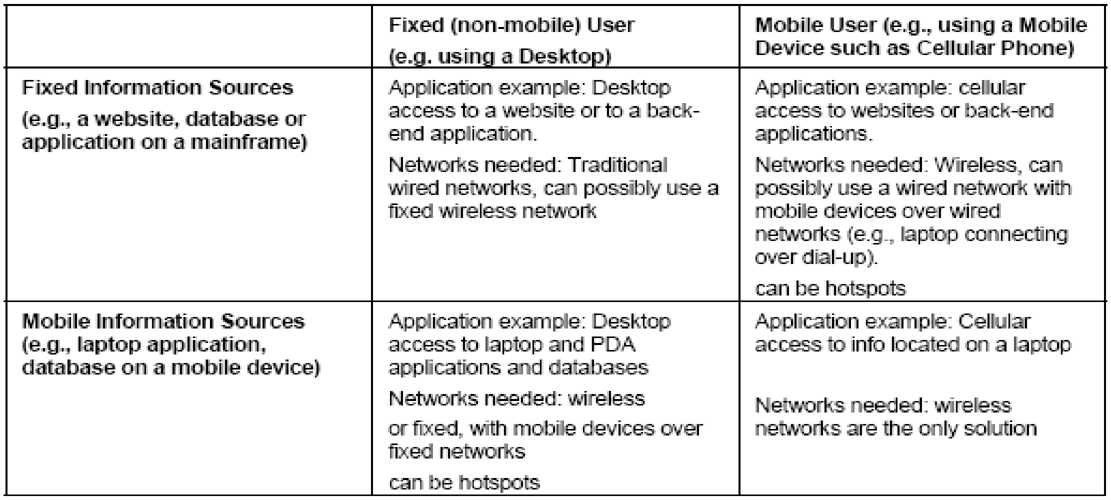
**Mobile B/G2B.** The major application in this category is the supply chain that can benefit from wireless enablement in several processes. These include purchasing, manufacturing, distribution, and customer service and sales. Different types of mobile technologies have been used in supply chains, ranging from bar code scanners to wireless sensors and RFID tags for improved data capture and asset management. In particular, handheld devices with Symbian and Windows CE operating systems connected with Wi-Fi LANs offer extensive opportunities for monitoring the supply chains at almost all points. Newer systems are using wireless sensor networks to detect any damages to the goods during transit and to alert the receivers and the senders for appropriate action.

### 2.2.2 Mobility of Users, Target Sources, and Networks

Mobile computing applications have to consider the mobility of users, target information sources, and the networks that interconnect them. Basically the following scenarios are possible:

- Users (mobile or fixed)
- Networks (mobile or fixed)
- Target information source (fixed, mobile)

Table 2-1 shows what type of networks are needed for mobile or fixed users/information sources. The applications for fixed users and fixed information sources are not mobile applications, while most of the mobile applications being developed at present are for mobile users who need access to fixed information sources. Although mobile information sources are relatively rare at present, this situation will be more common as more data and applications move to mobile devices. We can also add another dimension to this discussion. We have assumed that the programs are static even when the devices are mobile (i.e., the same programs are on your laptop when you travel around). We can now consider the mobility of code (known as ***mobile agents***) as another dimension. In this case, you could have the situation where your code is mobile but the device is not, and vice versa.



| | Fixed (non-mobile) User (e.g. using a Desktop) | Mobile User (e.g., using a Mobile Device such as Cellular Phone) |
|---|---|---|
| Fixed Information Sources<br>(e.g., a website, database or application on a mainframe) | Application example: Desktop access to a website or to a back-end application.<br>Networks needed: Traditional wired networks, can possibly use a fixed wireless network | Application example: cellular access to websites or back-end applications.<br>Networks needed: Wireless, can possibly use a wired network with mobile devices over wired networks (e.g., laptop connecting over dial-up).<br>can be hotspots |
| Mobile Information Sources (e.g., laptop application, database on a mobile device) | Application example: Desktop access to laptop and PDA applications and databases<br>Networks needed: wireless<br>or fixed, with mobile devices over fixed networks<br>can be hotspots | Application example: Cellular access to info located on a laptop<br>Networks needed: wireless networks are the only solution |

**Table 2-1: User Device versus Information Source Mobility**

### 2.2.3 Adding Other Capabilities (Positional, TV, and Voice) to Mobility

Mobile computing applications have several variants that could be called MPTV (mobile, positional, TV, and voice) services. In reality, many "M" applications are adding V (voice), P (positional, also known as location) and T (television) capabilities as value-added services.

We will use the term mobile computing application to imply one or more capabilities of MPTV, unless otherwise specified.

Mobile computing application = mobile + positional + television + voice

***Mobility capabilities*** describe the phenomenon of using wireless mobile devices such as digital phones and PDAs to search the Internet, access data and information, and conduct purchasing or business transactions. m-Commerce is fueled by the extreme popularity of mobile devices such as laptop computers, cellular phones, PDAs (personal digital assistants), and Palm Pilots.

However, the vast majority of devices and usage continue to depend on laptops and PCs, which may remain the de facto standard of devices used to access enterprise data and applications. Although the mobile PDA and telephone device markets are growing rapidly, the growth in the North American market is slower than in the European and Japanese markets.

***Voice capabilities*** are gaining in importance to support users who want to use telephones and other voice-driven devices for conducting e-commerce. For example, while driving or walking, it is easier to use a telephone than a computer. Technologies and standards such as Voice over IP (VoIP) and Voice Markup Language (VXML) will play a key role in v-commerce.

***Positional capabilities*** are providing support to the customers based on their geographic position (e.g., giving you information about deals in the Boston area when you are in Boston).

Many systems use a GPS (Geographical Positional System) to locate the position of the customers. But other approaches such as AoA (angle of arrival) are also becoming popular.

Most positional capabilities are becoming available as value-added location-based services (LBSs). See Section 2.8.1 for a discussion of LBS. .

***Television capabilities*** exploit another area of work that involves mobility. The idea is that you can use your TV to do Web surfing and online purchasing. For example, if you see an advertisement of a product on TV, you can then activate a purchase through your remote control. The TV set boxes will be programmed to support T-Commerce.

### 2.2.4 High-Level Architecture of Mobile Computing Applications

Before proceeding, let us take a quick look at a generic architectural view of EB applications shown in Figure 2-2. This architectural framework shows mobile computing applications as a multi-tiered client/server (C/S) model in which two integration layers surround the business logic. The front-end integration layer takes into account the wide range of mobile and fixed devices (laptops, Web browsers, PDAs, cellular phones) and applications (desktop or mainframe-based) that you need to communicate with. The back-end integration is used to connect to various local as well as remote (external trading partner) applications and databases). Notice that both integration layers are triangular; i.e., the integration glue is thin in some cases but quite thick in others. For example, integration with Web-based applications requires less effort than a mainframe-based application. The integration effort also depends on whether you are interacting with local (i.e., within the same enterprise) or external applications. This architecture can be used to study the interplays between the infrastructure components and to study integration/migration issues, and to address operational issues such as performance, fault tolerance, security, and manageability. We will use this architecture throughout this chapter as a framework to illustrate how various mobile computing applications can be viewed as specialization of this view. The reader should be reminded that the focus of this chapter is on applications and models and not on deep technical/architectural issues. The technical and architectural issues are mentioned only as sneak previews of what is covered in the balance of this book. In particular, see Chapter 11 for architectures of wireless systems.

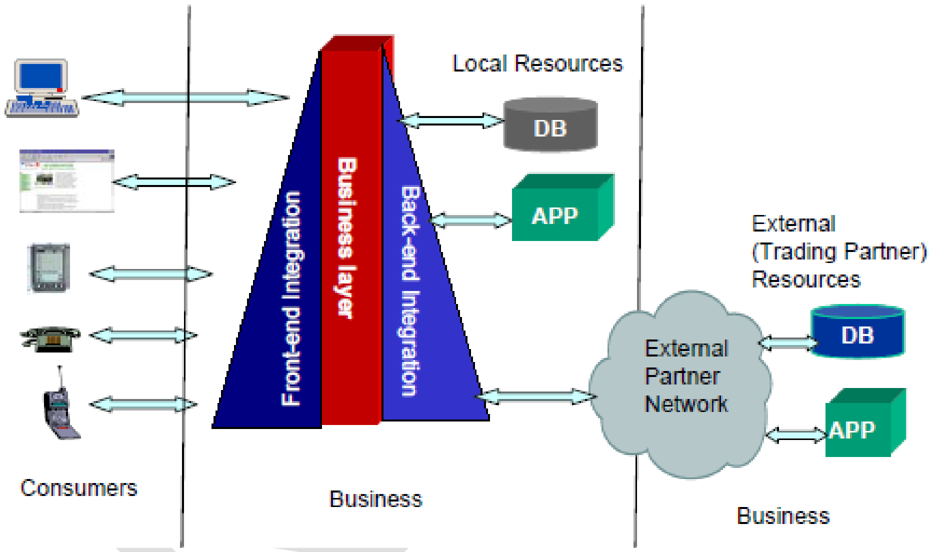


**Figure 2-2: High-Level Architecture of Mobile Computing Applications**

## 2.3 Messaging for Mobile Users

### 2.3.1 Short Message Service (SMS) – Wireless Text Messaging

The Short Message Service (SMS) allows users to send and receive text messages to and from their mobile telephones. The text can be comprised of words or numbers or an alphanumeric combination. SMS was created when it was incorporated into the Global System for Mobiles (GSM) digital mobile phone standard. A single short message can be up to 160 characters of text in length and contains no images or graphics. Although SMS is supported by cellular phones based on different cellular networks, most SMS services are supported by GSM providers. SMS is particularly good for “pushing” information to mobile phone users. In particular, SMS is used to push alerts, such as “new email from boss,” “meeting cancelled,” “appointment changed at . . .” etc. SMS can also be programmed to generate alerts from any data changes in corporate databases such as “supply chain is too slow,” “inventory levels have dropped below re-order points,” and “100 online purchasing items have been received.” SMS can also be used to pull data from a database, such as customer street address and fax number. For many of these types of applications, SMS supports a quick response. The main advantage of SMS is that it is simple and quick. The main disadvantage is that it is not meant to support conversational and interactive applications – it is an email service.

SMS has been a huge success in European GSM markets. It has also gained considerable ground in the United States. Instead of corporate efforts, the SMS market has been largely created via word of mouth. The user adoption has been phenomenal, especially in Europe, and has resulted in volumes of 2.5 to 3 billion SMS messages per month. According to the EMC for GSM Association, 2.4 billion messages were sent in May 2002. SMS is a huge success in several m-government initiatives around the globe because many citizens own cellular phones that support SMS. Thus SMS has become a vehicle to inform the public in many countries.

The primary benefit of SMS to the users is that they can use the same cellular phone for talking as well as short emails. In most cases, people use SMS just to scan the email header (“from” and “subject”) and send short replies like “I will get in touch within an hour.” Main SMS benefits include delivery of notifications and alerts, guaranteed message delivery, and ability to screen messages and return calls in a selective way. More sophisticated functionalities such as generation of messages are also available. Figure 2-3 shows the overall architecture of SMS.

The heart of SMS is a Short Message Service Center (SMSC) that directs all short messages to and from the mobile phone. The architecture is based on a store-and-forward model. The SMSC receives a message and directs it to the appropriate mobile device. Before sending the message, the SMSC finds the roaming customer by consulting "home location register (HLR)." The HLR part of a cellular network (in reality, HLR is part of a GSM cellular network), keeps track of a customer location. After receiving the request, HLR responds to the SMSC with the subscriber's status: inactive (phone turned off) or active (phone turned on). The SMSC transfers the message to the mobile device if active and receives verification that the message was received by the end user. If the user is "inactive," then the SMSC holds onto the message and attempts to deliver it when the subscriber turns on his/her device. There is some handshaking between the HLR and the SMSC when a user turns on his mobile device – the HLR detects this activity and sends a SMS notification to the SMSC. The SMSC software resides in the operator's network and manages the billing services. Many operators offer Web-based interfaces to their SMSC so that the users can send short messages to any mobile phone from the Web. Some websites offer free SMS.

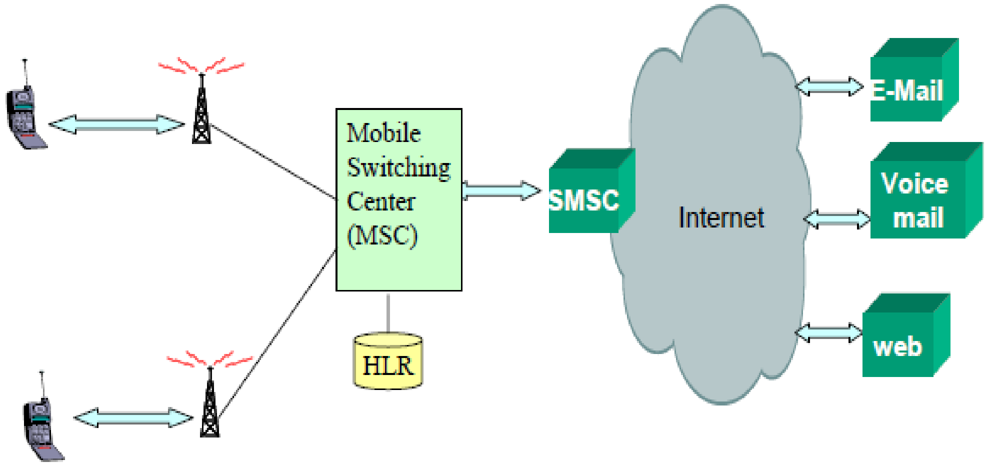


**Figure 2-3: SMS Architecture**

Users of SMS need the following:

- A mobile phone that supports SMS
- A subscription to a mobile telephone network that supports SMS (usually GSM)
- Knowledge of how to send or read a short message using the specific model of mobile phone
- A destination to send/receive messages. This may be another mobile phone, fax machine,

### PC or Internet address

An interesting characteristic of SMS is that a mobile handset can send or receive a short message at any time even when the user is talking. This simultaneous voice, data and fax activity is possible because short messages use the signaling frequencies that do not interfere with the radio channel used by voice and fax. SMS uses the signaling path to deliver shortburst data that carries its 160-byte messages. Thus, the users of SMS rarely get a busy or engaged signal. Due to the benefits of SMS, new applications are being developed. Examples include profile-editing, wireless points of sale (POSs), automatic meter reading, remote sensing, and location-based services. Additionally, integration with the Internet is leading to new applications such as instant messaging, gaming, and chatting. SMS has several benefits. It is very easy to install and use. Due to the guaranteed message delivery, polling is not needed and wireless bandwidth is not wasted. When the SMS provider sees that a user is connected and an SMS message is waiting in the SMSC for the user, the message is delivered. The main drawback of SMS is security because plain text can initiate an SMS message. Because anyone can send such a message, there is a possibility of false alerts. Overall, SMS is a useful and realistic notification service for applications such as email and voice mail.

### 2.3.2 Blackberry

BlackBerry®, from Research in Motion (RIM), is a popular wireless device that provides quick access to email, phone, SMS, organizer and Web applications. Based on a proprietary and patented system, BlackBerry is an integrated package that includes hardware, software and service, providing an end-to-end solution. It combines wireless handhelds with optional data and phone services and software that integrates with Microsoft® Exchange and Lotus® Domino™. Blackberry also provides end-to-end security with extensive encryption support. Recent versions of Blackberry handsets include an integrated speaker and microphone. Users of Blackberry can:

- Send and receive emails from anywhere
- Place a phone call while reading their email messages in a meeting
- Coordinate a meeting from the lobby of a hotel
- View information from a corporate database while traveling in a train

BlackBerry was designed to meet one major requirement – how to stay connected to one's desktop email and organizer information such as contacts, calendar, tasks and memos while in transit. A common solution has been to carry laptops to answer emails – a very cumbersome option. Typically, mobile professionals use a laptop when traveling and dial in to the corporate email server from a hotel room to read their email. Some use special software to send email notification to a pager or cell phone so they know what is in their inbox before bothering to dial in. Some people have used PDAs to dial in for email. But this is a risky option because of the lack of security software available for the PDAs. Technically, BlackBerry eliminates the need of dial-up by using a "push" model instead of the traditional "pull" model. In the pull model, the user connects to the corporate email server to check for new messages. In a push model, the email server automatically connects to the user and pushes the new email to the handheld. This provides always-on email service. BlackBerry does not use a separate email address for the wireless handheld.

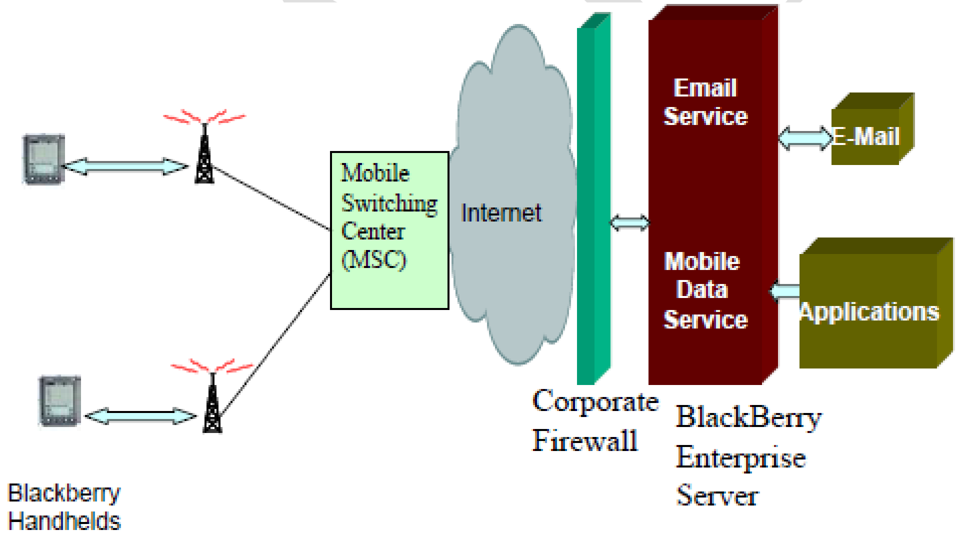


**Figure 2-4: Blackberry Architecture**

Figure 2-4 shows an overview of the Blackberry system architecture. The key pieces of this architecture are a) email server, b) the BlackBerry Desktop Software's Redirector component, c) the RIM Wireless Handheld and d) the wireless data network. The general operation of the system is as follows:

- Email arrives at the email server for the BlackBerry user
- The BlackBerry Desktop Redirector is then notified by the mail server. The Desktop Redirector retrieves a copy of the message, compresses and encrypts it and sends it via the Internet to the wireless network.
- The wireless network delivers the message to the handheld.
- At the handheld, the message is decrypted and decompressed and the user is notified of its arrival.

For this email redirection system to operate, users must leave their desktop computers running (a password-protected screen saver is recommended for security). The path from the handheld to the desktop follows the same steps, only in reverse.

### 2.3.3 Multimedia Messaging Service (MMS) for Wireless

While SMS, or text messaging, has been a huge success in Europe, MMS, mainly picture messaging, has been phenomenally successful in Japan. Simply stated, the Multimedia Messaging Service (MMS), as its name implies, is the ability to send and receive messages comprising a combination of mixed media including text, sounds, images and video to MMScapable handsets. Conceptually, MMS is a presentation layer for email that integrates multiple presentations from SMS, email, unified messaging and other services on a handset. MMS has been designed to provide a similar user experience to that of existing services such as SMS, but has been extended to include multimedia elements. It is a non-real-time service and uses a store-forward model similar to SMS. The main difference is that MMS is based on open standards such as WAP (Wireless Application Protocol) while SMS has some proprietary interfaces and architectures. MMS is an open wireless standard specified by the WAP forum for 3GPP (3rd Generation Partnership Project). 3GPP is the new worldwide standard for the creation, delivery and playback of multimedia over high-speed 3G wireless networks. Tailored to the requirements of mobile devices, 3GPP uses MPEG-4, the new standard for delivery of video and audio over the Internet. Although MMS is a 3G standard, network operators across Europe are deploying MMS over 2.5G networks using WAP as a means of transport. We will look at

WAP and 3G-2.5G wireless networks later. The MMS phones allow users to exchange messages including still pictures, animations and sounds.

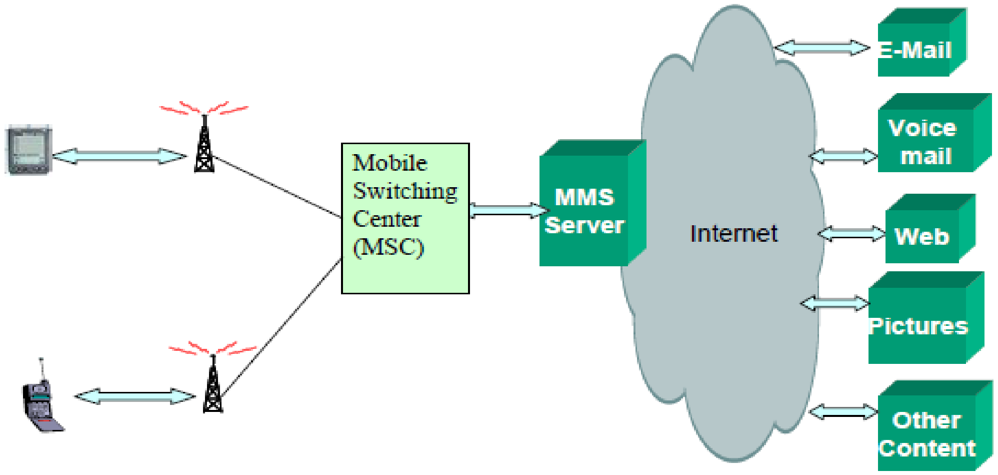


**Figure 2-5: MMS Architecture**

As shown in Figure 2-5, MMS is a store-and-forward protocol. Messages are stored on an MMS server, which sends the recipient a notification message using WAP Push (similar to an SMS message). The notification message triggers the receiving terminal to retrieve the message automatically (or depending on filters defined by the user) using the WAP GET command. This allows the receipt of the message to be transparent to the user, as is the case with SMS. To create an MMS message, a template is typically used to specify the relative position of any multimedia elements in the message. After creation, the message can be sent either to a phone number or email address. The message is sent to the user's MMS server, which either sends it to a phone (via a notification message) or converts it into a multi-part email and sends it to the recipient's email account. From a business perspective, MMS services could look very much like the i-mode service from NTT DoCoMo. For example, NTT DoCoMo earns about 10% of the total revenues from the i-mode services, and the content provider earns the rest (see www.mobileimode.com for more information). Thus content providers could do quite well in the MMS marketplace.

The content providers could provide still images such as photos, postcards, presentations, business cards, autographs, letters, telegrams, telexes and greetings cards. Entertainment could be another major content provider. In fact, many of the PC features and utilities (e.g., screensavers and plug-ins) could migrate over to the mobile phone, too. The content of MMS messages has been defined by the MMS Conformance Specification version 2.0.0 written by the MMS Interoperability Group. This group consists of representatives from CMG, Comverse, Ericsson, Logica, Motorola, Nokia, and Siemens. The MMS specification uses SMIL (Synchronous Multimedia Interaction Language) for the presentation format. SMIL is an XML-based standard from W3C that defines how the multimedia elements are coordinated. A great deal of information about MMS is available over the Web. Here are some key sources:

http://www.mobilemms.com
http://www.openmobilealliance.org
http://www.3GPP.org
http://www.forum.nokia.com/
http://www.ericsson.com/

**2.3.4 Applications of Messaging in m-Business, m-Government, and Mobile Life**

Wireless messaging services typically consist of:

- Basic email for mobile devices
- SMS text messaging
- Unified messaging
- Alerts and notifications to be sent and received by mobile devices
- Multimedia messaging services (future)

In business settings, many of these services are used regularly because they lead to improved productivity of employees, sales force, and field force (employees in the filed such as repair technicians). Different types of messaging services are popular in different parts of the world for business as well as personal use. SMS is extremely popular in Europe (being called the killer mobile application); Blackerry is quite popular in the US; and MMS is gaining popularity in Japan due to i-mode Very interesting applications of messaging services can be found in m-government. The State of Kentucky has initiated a Wireless Messaging Service (WMS) – an extension of the state’s Enterprise Shared Services Messaging Infrastructure that provides messaging services to over 35,000 employees in agencies throughout the state. The WMS solution involves a RIM wireless device, Blackberry software, and a Cingular wireless data network. In Singapore, "Mobile Service via SMS" allows library users to check accounts, renew items, pay outstanding fees/fines and receive reminders to return items. As another example, after the September 11 attack and the anthrax problems, all members of the US House of Representatives were issued a BlackBerry device to facilitate communications between members and appropriate authorities in case of an emergency. As yet another example, at the height of the SARS incident, the Hong Kong government sent a blanket text message to 6 million SMS users to warn against rumors and explain government plans.

### 2.3.5 Mobile Commerce – Buying/Selling Through Mobile Devices

**Overview and Examples**

M-Commerce describes the phenomenon of using mobile devices such as digital phones and PDAs to search the Internet, access data and information, and conduct purchasing or business transactions. m-Commerce is fueled by the extreme popularity of mobile devices. However, a large proportion of the usage continues to depend on laptops and PCs, which may remain the de facto standard of devices used to access enterprise data and applications

Wireless access to the Internet to surf the Net for bargains is becoming common. People can look for bargains while waiting in the doctor's office, having their car serviced, or on a fishing trip. M-Commerce is a competitive business. To stay in this business, companies need to provide more user-friendly, efficient, and secure transactions than their competitors. They may also need to include digital wallet services, ease of navigation, security, and context-relevant services. Another value-added service is handling of billing (see the sidebar, "Billing for MCommerce – A Thorny Issue").

- What is needed to make m-commerce a reality? Here are some ideas:
- Wireless networks. At present, 3G and Bluetooth are two top contenders.
- Middleware such as Wireless Application Protocol (WAP)
- Innovative new applications that are unique to mobiliy – for example, positional commerce (see next section)
- Wide use of handset devices to conduct business

**Why m-Commerce?** The wireless Internet has many features that permit mobile interactive services to be more personalized than traditional Internet applications.

**Mobile telephones** are carried by their owners almost everywhere and kept switched on most of the time. Consumers can thus not only gain access to wireless services wherever there is a network presence, but also keep tabs on time-critical information, such as stock market reports or urgent messages.

**Wireless-network operators** – at least those using the GSM standard – are uniquely able to determine the identity of a user. Since mobile telephones are not usually shared, and a personal-identification number often protects them, the telephone itself can be used as a means of identification. Operators can detect a user's exact location, enabling a whole range of new applications.

Let us look at online buying/selling to understand the implications and opportunities for mobile computing. Online purchasing includes consumers, buyers, and suppliers engaging in online trade and includes links to back-end systems for inventory updates and credit checking. As shown in Figure 2-6, the purchasing process consists of several steps that can be viewed in terms of pre-purchase, purchase consummation, and post-purchase activities. In the prepurchase activities, the users browse through various sites, compare prices, and select the online merchants they want to buy the goods from. Naturally, the use of handheld devices can have the most profound impact on these activities. The main issue is how the content is displayed on small devices with small display units. In the purchase consummation activities, the user may use a shopping cart and place an order by using a payment system. Naturally, the payment systems should work with mobile devices in this activity. The post-purchase activities involve the classical "back-end" systems that handle settling of payments, shipping and receiving, etc

M-Commerce involves a large number of systems that allow mobile users to search company catalogs for certain price ranges and then place orders for chosen product(s) through mobile devices. Needless to say, all these activities must be conducted securely through mobile devices over wireless networks. In addition, the order processing, inventory control, payment, and shipping/receiving systems are employed. All these systems need to work together to satisfy the demands of mobile buyers and sellers. Due to this demand, several specialized middleware services are needed to support mobile computing and online purchasing. These services are also being packaged with other infrastructure services to form ***"Middleware Platforms"*** that support mobility and ecoomerce**.** Examples of these platforms are ***Mobile Application Servers*** such as IBM's Websphere and Microsoft's Internet Commerce platform.

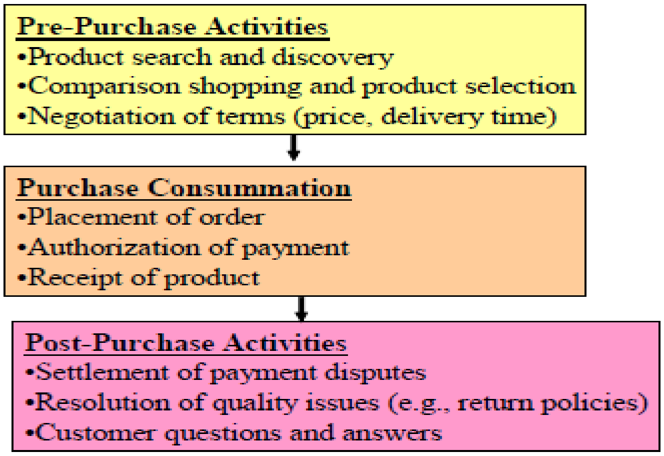

Pre-Purchase Activities
•Product search and discovery
•Comparison shopping and product selection
•Negotiation of terms (price, delivery time)
Purchase Consummation
•Placement of order
•Authorization of payment
•Receipt of product
Post-Purchase Activities
•Settlement of payment disputes
•Resolution of quality issues (e.g., return policies)
•Customer questions and answers

**Figure 2-6: Purchasing Steps**

### 2.3.5.1 Web Storefronts and Virtual Shops for Purchasing

Mobile commerce can be conducted through a variety of models. Web storefronts and virtual shops are the main alternatives. In both these cases, mobile access has been added as another capability.

**Web Storefronts.** Web storefronts use the Internet to market and sell products and services to a global audience of customers. Web storefronts are limited to one seller, i.e., they enable a seller to use the Internet to differentiate its product offerings, enhance customer service, and lower marketing, sales, and order processing costs. For example, a shoe store can develop a Web storefront that allows customers to purchase shoes over the Internet. As shown in Figure 2-7, storefronts support Web-based purchasing systems that allow users to search company catalogs for certain price ranges and then place orders for chosen product(s). This represents online buying/selling through a catalog using a shopping cart, electronic wallet, or similar tool. It includes both consumers purchasing goods and online buyers purchasing goods from a supplier. It can also include links to back-end systems for inventory updates and credit checking.

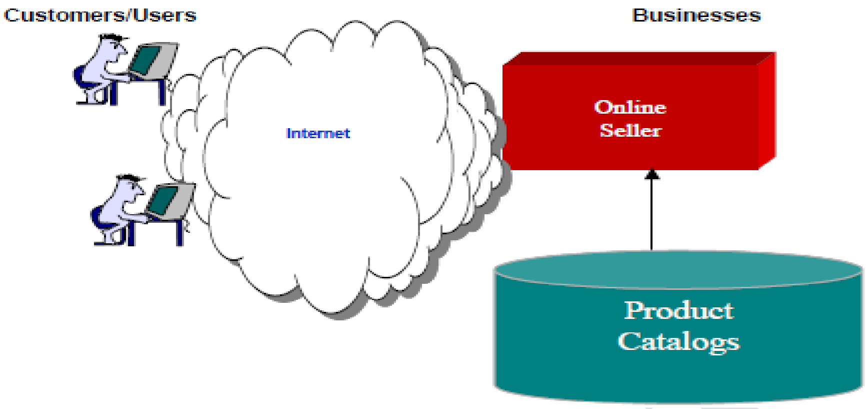


**Figure 2-7: Online Purchasing Through a Storefront**

A very large number of Web storefronts currently exist. Examples are:

- Staples.com – for buying office supplies online
- E-Bay – for buying numerous products
- Shop.com – for buying groceries
- Flowers.com – for buying flowers

Storefronts basically show a company's presence on the Web and are usually based on a product catalog that shows product features, price, expected delivery time, etc. These Webbased sales solutions deliver process and cost improvements to sellers but they are very "supplier-centric." These supplier-centric solutions can complicate efforts of customers to control expenditures and maintain preferred supplier relationships. For example, you may have to visit several storefronts to find a bargain.

**Virtual Shops.** Virtual shops go a step beyond the Web storefronts by providing a storefront that represents several back-end sellers. In other words, the restriction of a single seller is removed. For example, Amazon.com supports the purchase of books by tying several bookstores together. Enterprises that support virtual operations are known as "virtual enterprises" or extended enterprises. Basically, a ***Virtual Enterprise (VE)*** is a network or loose coalition of a variety of value-adding services in a supply chain, that unite for a specific period of time for a specific business objective, and disband when the goal is achieved.

Examples of virtual enterprises, in addition to Amazon.com, are:

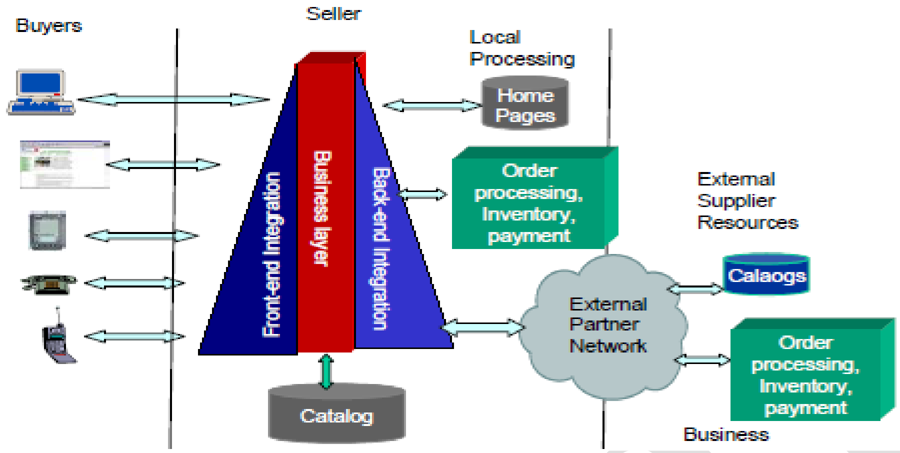
- Drugstore.com – for buying drugs online (many partners)

- Virtual Parts Supply Base (VPSB, http://www.vpsb.com/) – supplies hard-to-find parts for the US government
- The National Industrial Information Infrastructure Protocols (NIIIP) Consortium – develops inter-operation protocols for manufacturers and their suppliers (for more information on NIIIP see http://www.niiip.org).

Virtual enterprises can be customized, if needed, to reflect a buying organization's unique trading agreements, workflow, and business rules. These virtual procurement channels, also known as *e-procurement*, enable a self-service purchasing environment that pushes product selection and order initiation to the desktops of frontline employees through a common Web browser. Many early e-procurement solutions were intranet-based applications that did not fully leverage the ubiquity of the Internet. As a result, many e-procurement solutions are now transitioning to e-markets. Many unique issues in virtual shops and virtual enterprise arise. An example is customer care.

### 2.3.5.2 Variants of Mobile Commerce – Positional and Voice Commerce

Voice and positional commerce are becoming value-added features to m-commerce. Figure 2-8 shows a simplified view of variants of mobile commerce that includes C2B as well as B2B operations. The sellers provide wireless access to the main catalog and the order processing system. However, payment and inventory control systems are also involved in purchasing. In addition, the items not available at the seller can be provided by the other suppliers through their own catalogs and purchasing systems. Positional information can be useful in this context because if a user is calling from Boston, perhaps the Boston suppliers could be given a preference to save on shipping costs. Figure 2-9 takes a closer look at a positional and voice commerce applications. The wireless and wired devices (with and without GPS support) are connected to a Feature Server that consults a GIS (Geographical Information System) map for GPS support. The Feature Server also does interactive voice response, voice recognition, and speech generation. The Voice Portal provides voice menus or directories for users to select or traverse services. Based on this information, the back-end applications are accessed. These applications may reside in the Application Server that provides various transaction services (e.g. shopping carts, form requests) or may be part of a trader network.



Prototype, developed at the MIT Multimedia Laboratory. This prototype captures the sites you visit most frequently, e.g., your home, your office, your grocery store, and your bank. Then the items most relevant to the site where you are at present (or close to) are automatically retrieved and “spoken” to you. For example, if you are driving by the grocery store, the system will remind you that you need to buy groceries.

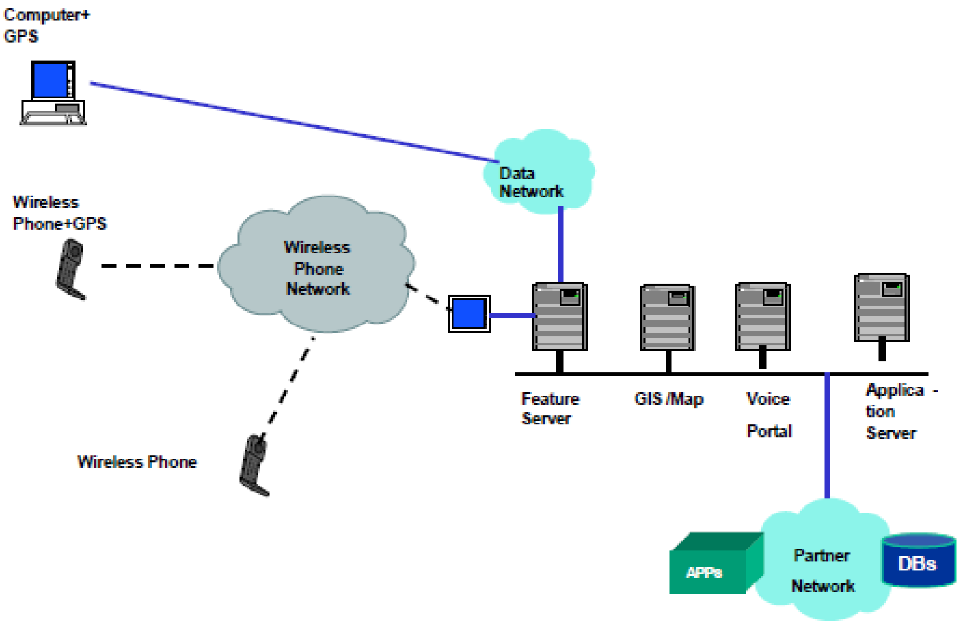


**Figure 2-9: Positional and Voice Commerce**

## 2.4 Mobile Portals

### 2.4.1 Overview and Examples

A mobile portal is a consolidated information channel for mobile customers. A variety of mobile portals have been created in the last few years. Here is a sample [Kalakotta 2002, Barnes 2003, Evans 2001]:

- DoCoMo in Japan is probably one of the best-known examples of mobile portals. The content providers allow millions of wireless users to access a wide range of content from i-mode cellular phones. We will look at i-mode in a later chapter.
- America Online’s AOL Anywhere makes AOL services universally available on a wide range of mobile devices including cell phones and TVs.
- Several companies such as Boeing’s “connexion” are trying to bring email and Web browsing to airline passengers. These portals in the sky will allow passengers to access their email and surf the Web while airborne.
- AT&T Wireless and other companies are creating voice portals where customers speak instead of click to obtain the information and services they need.
- GM offers a mobile portal called Virtual Advisor. This portal, built on a Hughes Electronics cellular and satellite system, offers voice-activated news, traffic information, email messages, and stock quotes over the Web.
- American Express has created a mobile portal to give cardholders a real-time and comprehensive view of their finances – accessible through wireless devices. The financial information is aggregated from cardholder relationships with banks, brokerages, mutual fund companies, and others.
- Starbucks is creating mobile portals in its coffee-houses so customers can browse the Net through their wireless laptops and PDAs.

### 2.4.2 What are Portals?

Since m-portals are extensions of portals, let us briefly look at portals. Simply stated, a portal is a website that serves as a doorway to a specific topic – they are intermediaries that offer an aggregated set of services for a well-defined set of users. Portals are reasonably popular in modern enterprises (they were very popular circa 1999). The oldest and perhaps still the bestknown portals are the Web search engines such as Yahoo and Lycos that allow users to search the websites for information. Over the years, the portals have evolved into websites that offer, in addition to Web searches, a broad array of resources such as email, forums, online shopping malls, and personalization tools. Advanced portals combine Web documents, databases, applications, visualization tools, search engines, integration technologies, speech recognition, and natural language processing to give users an integrated view. A mobile portal includes a set of integrated programs designed to make it easier for a mobile user to find information and, if needed, to conduct business or personal interest activities (e.g., shopping, setting up meetings, chatting). In addition to mobility support, these programs typically offer at least the following core features (see Figure 2-10):

- Web searching and Web advertising (e.g., home pages, banner ads, etc.)
- News about the topic of your interest
- Reference tools and specialized assistants ("wizards") to help with your chores (e.g., scheduling meetings, calendaring, video conferencing)
- Access to online shopping venues and, if needed, to back-end systems and services
- Some communication capabilities such as email, chat rooms

The purpose of all these integrated programs is to provide convenience, and a sense of community to the user, and to help make the user feel more comfortable about using the portal for the purpose of beginning his/her journey. So in this sense the portal is offering a valuable time-saving service. Of course, the purpose of the portal builder is to make sure that you conduct *all* of your activities by using the portal, thus capturing your "behavior" that could later be used for marketing. By offering visitors a portal to a specific topic, the portal vendor can control the results the user gets when he/she searches for a keyword. The links returned are the links that the portal vendor wants to return. By virtue of the free community building tools such as email, chat and forums, it also gives the visitor a way to communicate with the portal owner and ask questions and make comments about a specific topic. The advantage to the vendor, of course, is that by addressing these questions and comments, it gives the vendor an opportunity to become a trusted expert on a specific topic. Once a portal community has been established, then many suppliers may advertise on your portal about their product or service that relates to the community. This not only produces revenue for the portal vendor but again offers a valuable service to the visitors that keeps them returning to the portal site.

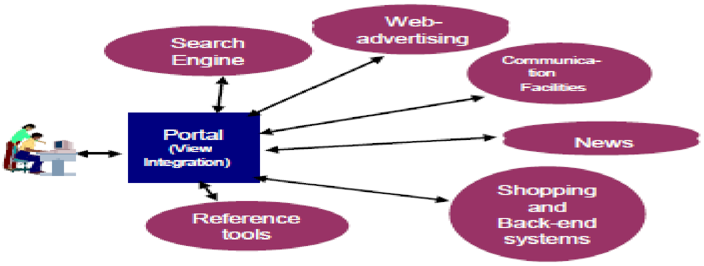

Search Engine
Web-advertising
Communica-tion Facilities
Portal (View Integration)
News
Shopping and Back-end systems
Reference tools

**Figure 2-10: Conceptual View of Portals**

### 2.4.3 What Are Mobile Portals? – A Closer Look

A mobile portal, as stated previously, is a repository with a set of integrated programs designed to make it easier for a mobile user to find information. In addition, these portals help wireless users to conduct business or personal interest activities such as calendaring, setting up meetings, chatting, shopping, etc.). Wireless technologies make portals into an on-call 24/7 service. Consider, for example, a physician that is paged to pay attention to a patient. Using a handheld device, the physician accesses an HMO (Healthcare Maintenance Organization) portal and pulls the patient information over a secure link. Similarly, a small business owner while traveling overseas gets a call from his secretary saying that some overdue taxes notice was served to the company main office. He accesses a small business portal for help with his taxes from his handheld device. Mobile portals can generate additional cash flow for several industries. To generate increased revenue, mobile portals must offer the ease of use and seamless functionality that improves the customer's quality of life. To be financially profitable, mobile portals must offer customers what they want, when they want it, and at a price that they accept. The key features are constant connectivity, time-sensitive information, location awareness, and ease of access to information accessed through mobile devices. Mobile portals are of two types. First are the portals that *contain content* about wireless and mobility. For example, www.thinkmobile.com is a portal for mobile users – it is a large repository of reports, case studies, and analysis of value to mobile users. Another example is the www.mobileinfo.com site – a large repository of reports, articles, products, and case studies about mobility. The others, of main interest to us, are the portals that are *accessed* through mobile devices. An example is the Mazingo Mobile/Wireless Portal (http://www.mazingo.net/mobile) that provides over 1200 sites formatted specifically for small-screen devices. Numerous other mobile portals exist. Some of these portals allow voice interactions, thus they are voice portals. In addition, positional information can be used. For example, a positional portal for weather will only show you the weather in the area that you are in. Naturally, conversion of existing Web portals to MVP (mobile, voice, positional) portals requires a great deal of work in conversion and delivery of the content to appropriate devices. Many consulting companies provide these services. For example, the HP Mobile Portal Solution is a consulting-led solution that delivers the software infrastructure, portal framework, mobile applications and the delivery team required to deploy mobile portals. The portal solutions usually portal component applications, from simple Web page displays to complex sequences of business events like location sensing, event notification, billing, and messaging. Business components employing Java, XML, and Visual Basic based on J2EE and .NET are usually employed in such solutions by consulting organizations.

**2.5 Special Mobile Applications (LBS, WSN, RFID)**

Several specialized mobile applications for specialized purposes are also being developed. Let us look at mobile agents and wireless sensor networks as examples. 2.8.1 Location-Sensitive Applications Many location-sensitive applications, also known as location-based services (LBSs), are being developed at present. Examples of these applications in m-business and m-government are:

- Search for the most relevant information according to your location – e.g., “I am looking for a shop within 5 miles of my home,” “what movies can I see in my neighborhood and how far will I have to travel,” and “find the nearest hotel and check what else there is in the neighborhood.”
- Display maps and calculate routes based on where you are located. In addition, you can improve transportation of goods by locating the nearest pick-up point and planning routes

based on real-time traffic situations; or by reporting alerts in case of changing traffic patterns, and adjusting the route.

- Some limousine companies are tracking their cars and can detect unauthorized off-route vehicle stops or off-route activities – for example, if a limo driver calls and says that he is at the airport but the LBS can show that he is at home (technology is not always good!).
- Advertising and notification services relevant to the user's location. For example, if a particular area has been declared hazardous, SMS messages could be sent to the citizens in the area.
- City Guides can be shown with location of nearby historical structures/buildings, government offices and interactive commercial services if you are in certain part of the city.
- Permit requirements can be obtained based on location. For example, permits for digging in an area with underground pipes or cables can be obtained easily. LBS also make it easier to obtain a drilling permit in a rural area and to register the associated filings with ground water districts and natural resources/environmental entities.
- Insurance risk analysis can be conducted based on locations. Tools such as Where@Risk, for example, provide a match of location to the appropriate risk criteria that can be used by insurance adjusters to develop policies. There are some additional developments worth mentioning in this regard.

The Telephone Number Mapping Working Group of the IETF is defining a DNS-based architecture and protocols for mapping a telephone number to a set of attributes (e.g. URLs) that can be used to contact a resource associated with that number. There are numerous applications that are driving the developments of LBS. The mobile operators are expecting significant revenues by offering a number of location-based services such as positional commerce. Location-sensitive information can be bundled into mobile commerce and other application as a value-added service. Regulatory agencies are also requiring mobile operators to provide accurate locations for emergency purposes and public safety (e.g., the E911 support). To meet these demands, a wide range of techniques for location management have been introduced. The oldest and by far the most commonly used technique is based on cell ID (i.e., a cellular user is located by the cell she is in). Other techniques include Assisted Global Positioning System (AGPS), Angle of Arrival (AOA), and variants of time taken (these techniques estimate distance by determining the time it takes for the signal to reach the user). These techniques yield different location accuracy (typical ranges are 50 meters to several kilometers).

### 2.5.1 Wireless Sensor Network (WSN) Applications

Sensors are small devices that can be used to measure temperature, humidity, motion, color changes in a painting, or any other measurable thing. These sensors, also called motes, are installed in particular locations or can be "sprayed" in a particular area to gather information. Sensors by themselves are not very powerful -- they just sit around and collect information. The real power of sensors comes wireless sensor networks (WSNs) which are formed when these tiny sensors start communicating with each other through wireless. WSNs can shuffle the information collected through thousands of sensors and transfer it to the public Internet or a corporate LAN. The information can finally be collected at a control point where it can be analyzed (Figure 2-15). Although most WSNs consist of very small processors communicating over slow wireless networks, WSNs can be used in several situations.

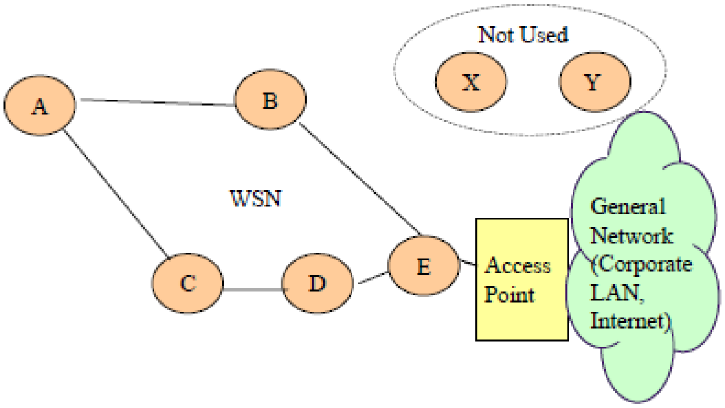


**Figure 2-15: A Sample Wireless Sensor Network**

Thousands of tiny low-power sensor devices are typically spread over large areas to form WSNs in many practical applications. The sensors of WSNs collaborate with each other to of the examples are:

- In many military situations, sensors are "sprayed" in a battlefield or an enemy area to detect and record certain activities and send information back to control centers for analysis and appropriate action.
- WSNs are being considered as an alternate to landmines where the sensors can detect enemy vehicles. This is much safer than landmines, which stay long after the conflict is over and are hazardous to the people living in that area. In contrast, sensors are harmless after conflict because they simply sit around collecting useless data until their batteries die.
- WSNs are also being used in medical situations for patient monitoring. For example, patient heart rate and blood oxygen levels are monitored by sensors. This information is gathered from different patients and sent to the PDA of an attending physician [Jovanov 2001].
- WSNs are being used in supply chain management systems also. For example, Sears Canada has completed an experiment that uses WSNs to detect if an item is damaged on transit before the customer gets it.

WSNs are also used to detect temperature fluctuations, earthquakes, automobile speeds, and cattle activities in fields. Many civilian applications of WSNs have been developed and deployed. See [Szewczyk 2004] for application of WSNs in habitat monitoring. WSN applications need specialized platforms. These platforms, discussed in more detail in Chapter 4, provide a hierarchy of services that range from low level sensors to higher level data aggregators, and data storage and analysis capabilities (see [Hill 2004]).

### 2.5.2 RFID Applications

RFID (Radio Frequency Identification) systems have been used in a variety of applications. An RFID system typically consists of the following components:

- A tag or label that is embedded with a single chip computer and an antenna. The antenna is so small that it can be printed on the tag with carbon-based inks. RFID tags (chip plus antenna) are also called "transponders." The tag is somewhat similar to the commonly used bar code labels. However, an RFID tag has more intelligence. Tags are of two types.

"Passive" tags, the type of tags commonly used in retail stores and supply chain systems, pick up enough energy from the radio to operate and to communicate back to the radio. "Active" tags have an embedded battery and offer the advantage of longer-range communications and can communicate with other tags. In this case, a WSN can be formed between the RFID tags.

- A short range radio (e.g., a wireless LAN such as Bluetooth) that communicates with the tag. The radio receiver is usually an RFID reader, or detector/interrogator., that gets the information from the RFID tag and then may send it to a back-end system for processing.

An RFID system's "read range" — the distance a tag must be from the detector/reader — varies from a few centimeters to tens of meters, depending on frequency used, whether a tag is active or passive, and the type of antenna used on the reader. In many practical applications, an RFID reader transmits a wireless signal to the RFID transponder, which responds in milliseconds with a unique identification code sent to the reader. The reader sends this code to the host system for processing. RFID is being used increasingly instead of the old bar-code systems because unlike bar code-based tracking systems, an RFID system can read the information on a tag without requiring line of sight and without the need for a particular orientation. That means RFID systems can be largely automated, reducing the need for manual scanning. In addition, RFID tags hold much more data than the bar code labels. In many areas, RFID-based passes are used in highway toll booths for automobiles. For example, in New Jersey, an EZPass system is being used heavily on the NJ Turnpike. An EZPass is bought and is pasted on the front windshield of a car. When the car approaches a toll booth, it slows down so that the RFID reader on the toll booth can read the EZPass number. As soon as this is done, the reader posts this transaction to a database and then gives a signal to the toll booth that gives the green light to the automobile. The auto owner gets a monthly bill from EZPass for all the transactions. This whole process takes less than a minute – usually the car just slows down. In the older manual system, an auto driver gets a toll ticket when she gets on the NJ Turnpike, then before exiting, the driver stops, takes out her ticket, gives it to the toll booth attendant, pays the attendant, and then leaves. This may take several minutes. Similar systems are operational around the globe at present.

Many airlines are using RFID for airline baggage tracking. For example, British Airways has trialed a paper label-based RFID transponder. Each luggage has an RFID tag that is read by the RFID readers as the luggage moves on the belts. By using this system, more than 225,000 pieces of luggage were transferred successfully between airport hubs from Manchester and Munich to London's Heathrow Terminal 1 with 100% accuracy. RFIDs are also used in tracking valuable assets. Unique RFID tags are installed on the asset and can be detected by RFID readers. If stolen, law enforcement agencies could be informed of the RFID serial numbers. For highly valuable assets, this information can be used for random checks at ports and other exit points within a country, thus preventing the asset from leaving the country. Additional information about RFID can be found at www.rf-id.com.

## 2.6 Mobile Agent Applications

### 2.6.1 What are Mobile Agent Applications?

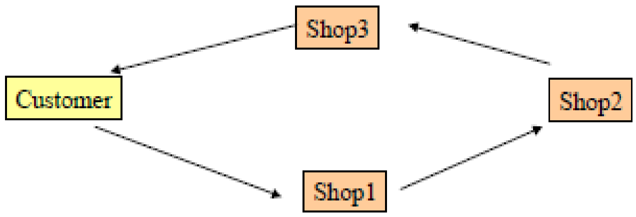
Mobile agent applications represent a different class of applications in which the application programs themselves are mobile. Most of the mobile computing applications discussed so far use mobile devices over, typically, wireless networks. But the application code itself does not move around – it either resides on the handset, the back-end system, or both. In case of mobile agent applications, mostly implemented through Java code, the application code may itself migrate from the back-end system to your handset and then move to another site.

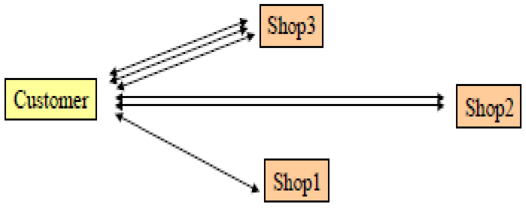
***Mobile agents,*** as stated in Chapter 1, are programs capable of being transferred to remote hosts in order to carry out different tasks on behalf of their users. Mobile (transportable) agents have the ability to travel through the network and carry out a set of operations on behalf of a user (customer) -- they do so with some degree of autonomy to satisfy its user's goals. A mobile agent can halt its execution, move to another host on the network while maintaining its state, and resume execution on the destination host. Mobile agents are also typically intelligent, known as mobile intelligent agents (MIAs), and thus have the ability to learn, use knowledge effectively, and adapt to new situations. An example of mobile intelligent agents is a ***"shopbot"*** that moves around a trading network to shop on our behalf by using certain level of intelligence in looking for bargains. Thus a mobile intelligent agent is typically:

- *Transportable:* moves from one site to another
- *Knowledgeable:* has knowledge of a domain (e.g., insurance) and user needs
- *Self-learning:* can acquire additional knowledge from different situations
- *Pro-active*: takes initiative; sets and pursues goals
- *Autonomous*: decides what to do without external human intervention
- *Timely*: does not spend forever deciding what to do next
- *Persistent*: remembers a "lifetime" of activity
- *Social and communicative*: interacts with other agents

### .2.6.2 Mobile Agents Versus Client/Server Model

Mobile agents basically provide an alternative to the very common client/server model. In a client/server model, the clients send the data to the program sites (servers) and receive the results. In a mobile agent model, the program is shipped to the data sources -- it thus travels from one data source to the next, collects the results, and sends the results back to the originator. Figure 2-16 illustrates the differences between client/server and mobile agents by using a shopping example. Suppose you wanted to find a cheap computer quickly. In the client/server model, the customer issues calls to different shop sites, in some cases multiple calls are issued to the same shop, and the results are sent back to the customer after visit to every shop site. In a mobile agent model, a "shopbot" is sent to the first shop where it checks for the desired computer. It then moves to the next shop (carrying the results from shop1). After shop2, the shopbot moves to shop3, carrying the results from shop1 and 2. The accumulated results are sent back to the customer after shop3.





a) Shopping by using a Client/Server Model b) Shopping by using a Mobile Agent Model

**Figure 2-16: Mobile Agent Versus Client/Server Model**

Which model is better. Well, it depends. First, let us consider the network considerations. The client/server (C/S) model assumes a sustained network connection to carry the requests and responses. If numerous network calls need to be issued to a server, then the C/S model consumes a great deal of network resources. On the other hand, the mobile agents migrate from site to site and do not consume network bandwidth to carry multiple request/reply packets. Mobile agents are particularly suited for wireless networks because they do not need a sustained network connection, i.e., the customer can ship an agent and disconnect -- it can later connect to receive answers. Second, let us consider the programming complexity. In the C/S model, the intelligence is at the client machine because the decisions are made at the customer location. On the other hand, mobile agents have to carry a great deal of intelligence with them -- they basically accumulate results and roam around the network making decisions on behalf of the customer. Mobile agents can decide dynamically where and when to travel to a particular destination site based on some embedded mobility metadata to perform some required work. Mobile agent technologies grew out of three earlier technologies that have attempted to address the limitations of the classical RPC (remote procedure call) model of C/S systems. These technologies include process migration where the entire address space is moved from one site to the next, remote evaluation programming where only the needed program (not the entire address space) is shipped from one site to the next, and the mobile objects where the executable code and data with state information are shipped from one site to next. See [Wong 1999] for a detailed discussion of these variants of mobile agents. In general, the current mobile agent technologies are outgrowth of mobile object systems, mainly Java, through refinements and addition of capabilities such as autonomy and intelligence (mobile objects may or may not be autonomous or intelligent).

### 2.6.3 Sample Applications of Mobile Agents in Mobile Computing

Although the mobile agent technologies have been around for a while, real life applications are relatively sparse. We have already discussed shopbots that are mobile intelligent agents which go around and shop on your behalf. Mobile agents are suitable for wireless networks. For example, an agent can move from site A to site B in a wireless network, disconnect from the wireless network, do local processing at B, then connect to the network for migrating to site C, disconnect, etc. This cycle of process, connect to migrate, migrate, disconnect, and process can be followed as the mobile agent goes around the network. This will work well in a slow wireless network. Let us consider a more detailed example of this. A company that needs to order office supplies could use agents ("inventory agents") to monitor the quantity and usage patterns of office supplies within the company and launch buying agents when supplies are low. The buying agents can roam around the network, automatically collecting information on suppliers and products that fit the company needs. They can also decide which suppliers and products to investigate in detail, negotiate the terms of transactions with selected merchants, and finally place orders and make automated payments. In this example, the inventory agents may or may not be mobile but the buying agents should be mobile. Other but similar applications of mobile agents in Ecommerce are:

- Personal agents to go around the network to collect and present information to you in the way you want it (e.g., sort the sites you want to visit in terms of historical significance)
- Mobile automated negotiators for retail e-commerce, bandwidth trading, subcontract for manufacturing, electronic trading of financial instruments, and vehicle routing among independent dispatch centers. These automated hegotiations can be conducted from a cellular phone through mobile agents. The cellular phone just invokes a mobile agent, disconnects from the network, and the mobile agent hops around the network (wired or wireless) negotiating on your behalf.
- Collaborative agents that can serve as the mediators in manufacturing supply chains. These agents can monitor the status of supply chains, detect delays, and find alternative sites in case of failure/unacceptable delay of a supplier. Supply chain systems of this type are proactive in nature and are known as "Zero Latency Supply Chains" because they can detect and correct problems without any delays (hence zero latency).
- Multi-agent systems for large scale trading and brokering that involve many local agents (some static, some mobile). Local agent managers handle local agents and multi-agent systems handle multiple local agent managers. Examples of multiagent systems can be found in the energy market where multiple energy suppliers can have their own local

agents coordinated by multi-agent systems and the manufacturing segment for manufacturing resource planning.

### 2.6.4 Mobile Agent Requirements

Mobile agent systems must satisfy the following requirements:

**Portability.** Mobile agent code itself must be portable; when an agent arrives at a server the server needs to be able to execute that agent. Commonly used computer languages such as C and C++ are not very portable. Compiled C code only works on the machine it was compiled for and the source form is notoriously unportable. Portability can be achieved by running computer programs inside virtual machines interpreters, but overhead has limited the use of interpreted languages. Most mobile agent systems under development now rely at least in part on virtual machines to standardize the execution environment.

**Ubiquity.** In order for mobile agents to be successful they need access to many different computer resources. Servers for agents must be commonplace; there needs to be a widely accepted framework for executing mobile agents deployed on many machines across the Internet. In practice the requirement of ubiquity means that the execution environment needs to have market acceptability, be freely available, and be unencumbered by restrictive intellectual property requirements.

**Network Communication**. Mobile agents that live in the network need to be written in a language that makes network access simple. It must be easy to transfer objects across the network and to invoke methods of remote objects. Traditional computer languages treat networking structures as an afterthought, usually providing only a minimal socket library. Languages that better support network access have typically not been widely used. This situation is improving with the current development of language-neutral distributed object frameworks such as CORBA.

**Server Security**. A major concern specific to mobile agents is the protection of the servers running the agents. Running arbitrary programs on a machine is dangerous: a hostile program could destroy the hard drive, steal data, or do all sorts of other undesirable things. This risk must be thoroughly addressed if mobile agent environments are to succeed. Two types of security are possible to protect servers from malfunctioning and hostile agents: physical and social.

- Physical security refers to building servers for agents in such a way that the agents cannot harm the server. The ``laws of physics" of the server execution environment can be designed to make dangerous operations difficult or impossible. Common approaches involve creating a ``sandbox" for visiting agents, restricting access to resources (preventing disk writes, for instance) and ensuring the agent cannot escape those restrictions. This approach to security is attractive; when it works, it is entirely effective. But the viability of physical security in the face of design complexity and server implementation bugs is unclear. In addition, physical security is typically focussed on protecting some underlying aspect of the server from the sandbox the agent is trapped in. But if multiple agents are put in the same sandbox how can the server guarantee that one agent cannot harm another? As we put more trust in the computations that take place inside sandboxes, the security of those sandboxes themselves becomes important.
- A second approach to server security is using social enforcement mechanisms to punish the creators of harmful agents. If a server administrator can find out who is responsible for a malicious agent, then that person can be held accountable via social mechanisms (such as lawsuits). Digital signature technology makes identifying the authors of agents possible. But there are limitations to a purely social approach to security. It may not be clear which agent is responsible for damage, nor will it be easy to determine ahead of time which agent authors are trustable. In practice some combination of social and physical enforcement of server security will be useful.

**Agent Security**. The complement of server security is agent security: whether the agent can trust the server on which it is executing. A mobile agent might contain secret information such as proprietary data and algorithms. Worse, servers might have an incentive to subvert the computation of a visiting agent. In the Internet-based DES cracking effort currently under design a major concern is protecting the computation from sites that pretend to do pieces of the problem but return false answers [Tre96]. Physical security answers to this problem are difficult. Secure, trusted hardware on the server could guarantee agent safety but is unlikely to be widely deployed. Agent programmers can protect their agents by obfuscating their code and verifying the results of the remotely-performed computation but the general applicability of these techniques is unknown. Social solutions may be possible in the form of reputation systems for servers. This area of security has largely been unexamined.

**Resource Accounting**. If economic control and incentive are going to be factors in net-wide resource use some mechanism to account for the resources that an agent uses and a way for receiving payment for those resources is necessary. In theory these requirements are not difficult to meet. Servers can keep track of the resource usage of agents, explicitly accounting CPU, memory, bandwidth and disk usage. Digital cash systems can be used to pay for services. In practice, these technologies are not widely deployed and the overhead they impose presents an engineering challenge.

### 2.6.5 Existing Mobile Agent Platforms and Architectures

Many mobile agent environments have been developed to satisfy these requirements in industrial sectors as well as the academic communities. We will list a few in Section 2.9.5.2. Although the environments vary widely, most current mobile agent environments are based on Java due to its portability and mobility features. The Java-based mobile agent environments use an architecture that is somewhat generic.

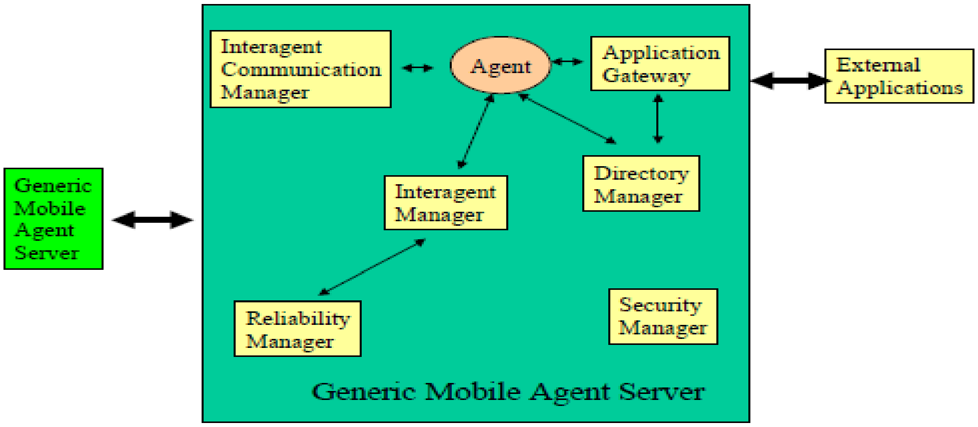
**Generic Architecture of Mobile Agent Environments**

The Java-based mobile agent environments use an architecture that is somewhat generic.

Figure 2-17 shows a generic mobile agent architecture discussed by [Wong 1999] that can be used as a framework for discussion. This architecture shows six different components:

- The agent manager is responsible for sending and receiving agents to/from remote hosts. It serializes the agent and its state before sending it to remote hosts and also deserializes and receives the agents on the other end.
- The reliability manager makes sure that the sent agent is properly received by the remote host. It also guarantees the persistence of state associated with agents.

- The security manager authenticates the agent before it is allowed to execute at the receiving host. All other mobile agent system components interact with the security manager to authenticate and authorize mobile agents.
- The application gateway provides secure interactions with external applications (nonagent) such as purchasing systems and product catalogs.
- The directory manager keeps a directory of all agents in the network.
- The inner-agent communications manager is responsible for managing communications between multiple agents that are dispersed throughout a network. . . .



**An important implication** of this architecture is that a mobile agent server must exist at each site where the mobile agent is supposed to run, Thus if you have a network with 100 hosts but only 7 have the mobile agent server, then your mobile agent can only roam around the 7 hosts. In addition, mobile agent systems are not interoperable (so what is new!). Thus if you are using the Aglet mobile agent system, then the aglet mobile agents can only run at the sites where the Aglet server is running.

## POSSIBLE QUESTIONS

## UNIT II

### PART-A (Online Examinations)

### PART-B (5 X 6 = 30 Marks)

### (Answer ALL the Questions)

1. Discuss about mobile agent applications with a neat diagram.

2. What are the key characteristics of mobile computing applications? Explain.

3. Discuss about mobile agent applications with neat diagram.

4. What are the key characteristics of mobile computing applications? Explain.

5. What is mobile portal and what are its main characteristics? Explain through a real life example.

6. Explain in detail about wireless messaging services.

7. Elaborate on Mobile portals with example.

8. Discuss about mobile agent applications with neat diagram.

9. What are mobile agents and what possible role can they play in m-business and m-Government? Give some real-life examples of mobile agent.

10. Explain in detail about wireless messaging services.

### PART-C (1 X 10 = 10 Marks)

1. Discuss the role of Mobile agent applications with example.
2. What are web services and mobile web services and why are they important to wireless web?
3. Discuss the role of HiperLAN2.
4. Discuss in detail about 3G cellular systems.
5. Explain in detail formatting output in WML.
6. Give the structure of table in WML and explain with example.

**KARPAGAM ACADEMY OF HIGHER EDUCATION**
**Coimbatore - 641021.**
**(For the candidates admitted from 2019 onwards)**

**DEPARTMENT OF COMPUTER SCIENCE,CA & IT**

**WIRELESS AND MOBILE COMPUTING - 19CSP105A**

**UNIT II :(Objective Type/Multiple choice Questions each Question carries one Mark )**
**PART-A (Online Examination)**

| S.NO | QUESTIONS | OPTION 1 | OPTION 2 | OPTION 3 | OPTION 4 | KEY |
|---|---|---|---|---|---|---|
| 1 | RIM means | Research Inner Method | **Research In Motion** | Research In Method | None of these | **Research In Motion** |
| 2 | MSC means | Movement Switching Center | Mobile Switch Center | **Mobile Switching Center** | None of these | **Mobile Switching Center** |
| 3 | Mobile portal is a | Connection channel for mobile customers | Consolidated channel for all | Consolidated channel for specific users | **Consolidated channel for mobile customers** | **Consolidated channel for mobile customers** |
| 4 | Examples for mega/super portals is | **Yahoo** | E-LOAN | eBay | None of these | **Yahoo** |
| 5 | Examples for vertical portals is | Yahoo | **E-LOAN** | LYCOS | None of these | **E-LOAN** |
| 6 | Enterprise portals called as | Corporate Portals | Transaction Portals | **Both a and b** | None of these | **Both a and b** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | PDA means | Personnel Device Assistant | Personal Digital Annexure | Personal Device Assistant | **Personal Digital Assistant** | **Personal Digital Assistant** |
| 8 | Sensors also called as | **Motes** | Devices | Firmware | None of these | **Motes** |
| 9 | RFID means | Radio Frequency Identifier | **Radio Frequency Identification** | Radio Free Identification | None of these | **Radio Frequency Identification** |
| 10 | RFID tags consists | Chip | Antenna | **Both a and b** | None of these | **Both a and b** |
| 11 | RFID tags also called as | Chip | Transceivers | Transports | **Transponders** | **Transponders** |
| 12 | Mobile agents is a | **Set of programs** | Set of hardware components | Firmware | None of these | **Set of programs** |
| 13 | MIAs is a | Mobile Interactive Agents | **Mobile Intelligent Agents** | Mobile Intellectual Agents | None of these | **Mobile Intelligent Agents** |
| 14 | Large number of collection of TCP/IP Networks are called as | Intranet | **Internet** | Both a and b | None of these | **Internet** |
| 15 | Network interconnectivity devices are | Routers | Gateways | **Both a and b** | None of these | **Both a and b** |
| 16 | IP means | **Internet Protocol** | Intranet Protocol | Interactive Protocol | Interconnect Protocol | **Internet Protocol** |
| 17 | DNS means | Domain Navigation Service | **Domain Name Service** | Domain Name Server | Domain Name System | **Domain Name Service** |
| 18 | WAIS means | **Wide Area Information Servers** | Wide Area Information Service | Wireless Area Information Servers | None of these | **Wide Area Information Servers** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19 | SMTP means | Simple Mail Transmission Protocol | **Simple Mail Transfer Protocol** | Simple Mail Transfer Protocol | None of these | **Simple Mail Transfer Protocol** |
| 20 | Telnet provides | Terminal access to Terminals | Hosts access to Terminals | Hosts access to Hosts | **Terminal access to hosts** | **Terminal access to hosts** |
| 21 | URL means | **Uniform Resource Locator** | Uniform Resource Location | Uniform Resource Loader | Unified Resource Locator | **Uniform Resource Locator** |
| 22 | WAP means | Wireless Application Process | Wired Application Protocol | **Wireless Application Protocol** | None of these | **Wireless Application Protocol** |
| 23 | FTP means | **File Transfer Protocol** | File Transmission Protocol | Fax Transfer Protocol | None of these | **File Transfer Protocol** |
| 24 | The following tool is a well known interface for the Internet | Email | **Gopher** | FTP | SMTP | **Gopher** |
| 25 | The users resides on the machine which has an IP address called | Immediate Internet Users | Active Internet Users | Indirect Internet Users | **Direct Internet Users** | **Direct Internet Users** |
| 26 | The users remotely log on the machine<br>which has an IP address called | Immediate Internet Users | Passive Internet Users | **Indirect Internet Users** | Direct Internet Users | **Indirect Internet Users** |
| 27 | Web Server consists of | Set of firmware | **Set of Programs** | Both a and b | Set of hardware | **Set of Programs** |
| 28 | The program that access non-web contents are called as | **Gateways** | Routers | Both a and b | None of these | **Gateways** |
| 29 | PC based web browser is | Netscape Navigator | Internet Explorer | **Both a and b** | None of these | **Both a and b** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 30 | ISP means | Intranet Service Provider | Internet Selection Provider | **Internet Service Provider** | None of these | **Internet Service Provider** |
| 31 | The first GUI browser is | Netscape Navigator | Internet Explorer | Both a and b | **Mosaic** | **Mosaic** |
| 32 | CGI means | **Common Gateway Interface** | Communication Gate Interface | Communication Gateway Interface | None of these | **Common Gateway Interface** |
| 33 | The following user connection is terminated each time when the user moves to new location | Mobile User | Internet User | Desktop User | **Nomadic User** | **Nomadic User** |
| 34 | The following user connection is not terminated each time when the user moves to new location | **Mobile User** | Internet User | Desktop User | Nomadic User | **Mobile User** |
| 35 | NSP means | **Network Service Providers** | Netware Service Providers | Network Service Programmers | Network Selection Providers | **Network Service Providers** |
| 36 | IAP means | Intranet Access Programmers | Internet Access Programmers | **Internet Access Providers** | Intranet Access Providers | **Internet Access Providers** |
| 37 | POP means | **Point of Presence** | Point of Point | Position of Presence | None of these | **Point of Presence** |
| 38 | An ISP offers the following services | Email services | Web hosting | Web services | **Both a, b and c** | **Both a, b and c** |
| 39 | An ISP provides | **IP address** | URL address | Both a and b | None of these | **IP address** |
| 40 | Routers are | **Software Programs** | Set of Hardware | Firmware | None of these | **Software Programs** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 41 | Routers are responsible for routing messages between | Hosts | **Networks** | Hosts and Networks | None of these | **Networks** |
| 42 | The physical networks are called as | Physical Group | **Subnets** | Internet | Super nets | **Subnets** |
| 43 | IP address is a | 8-bit number | 16-bit number | 64-bit number | **32-bit number** | **32-bit number** |
| 44 | During wireless transmission the basic unit of information is called as | Data | **Datagram** | Information | Packet | **Datagram** |
| 45 | ICMP means | Internet Control Message Program | Internet Control Method Protocol | **Internet Control Message Protocol** | Intranet Control Message Protocol | **Internet Control Message Protocol** |
| 46 | Mobile device assign to a particular network is called as | **Home Network** | Foreign Network | Fixed Network | Wireless Network | **Home Network** |
| 47 | Mobile device has to moved to another network is called as | Home Network | **Foreign Network** | Fixed Network | Wireless Network | **Foreign Network** |
| 48 | The Mobile node uses a ________ procedure to identify the home and foreign agents | Location | Selection | Seek | **Discovery** | **Discovery** |
| 49 | The datagram is encapsulated in an outer IP datagram is called as | Network | **Tunneling** | Fixed Network | Wireless Network | **Tunneling** |
| 50 | GRE means | Generic Routing Exchange | Global Routing Encapsulation | **Generic Routing Encapsulation** | None of these | **Generic Routing Encapsulation** |
| 51 | _________ is a gateway between Internet and mobile devices | **Protocol Adaptors** | Router | Wireless Gateway | None of these | **Protocol Adaptors** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 52 | _________ is used to translate the requests from wireless network to the web protocol stack. | Router | Gateway | **Wireless Gateway** | Wired Gateway | **Wireless Gateway** |
| 53 | Translate web contents into compact encoded formats by using | **CGI Scripting** | Router | Wireless Gateway | None of these | **CGI Scripting** |
| 54 | PICS means | Program for Internet Content Specification | Platform for Internet Control Specification | Platform for Intranet Content Specification | **Platform for Internet Content Specification** | **Platform for Internet Content Specification** |
| 55 | P3P means | Platform for Privacy Program | **Platform for Privacy Preferences** | Program for Privacy Preferences | None of these | **Platform for Privacy Preferences** |
| 56 | SMIL means | Synchronous Mobile Interface Language | Synchronous Multimedia Interface Language | Synchronous Mobile Interaction Language | **Synchronous Multimedia Interaction Language** | **Synchronous Multimedia Interaction Language** |
| 57 | DOM means | **Document Object Model** | Document Object Method | Data Object Model | Database Object Model | **Document Object Model** |
| 58 | WML means | Wired Markup Language | **Wireless Markup Language** | Wireless Mark Language | Wired Mark Language | **Wireless Markup Language** |
| 59 | MathML means | Mathematical Mark Language | Math Markup Language | Mobile Markup Language | **Mathematical Markup Language** | **Mathematical Markup Language** |
| 60 | DTD means | Document Type Data | Document Type Definition | **Document Type Declaration** | Data Type Declaration | **Document Type Declaration** |

## UNIT-III

## SYLLABUS

**Wireless Internet Mobile IP and Wireless Web** - Internet and Web – How it works – Mobile IP – WWW for wireless – Mobile Web Services - **Mobile Computing Platforms** - Introduction – Wireless Middleware – Wireless Gateways and Mobile Application Servers – WAP – I-MODE Wireless JAVA MMIT and BREW – Voice communication

## Wireless Internet, Mobile IP and Wireless Web

### 3.1 Internet and the Web: A Quick Refresher

### 3.1.1 Internet, Intranets, and Extranets at a Glance

Technically speaking, the Internet is a network based on the TCP/IP protocol stack. At present, the term *Internet* is used to refer to a large collection of TCP/IP networks that are tied together through network interconnectivity devices such as routers and gateways. The term *cyberspace*, first introduced through a science fiction book by Gibson [1984], has been permanently transferred to our vocabulary. It represents thousands of computers and computer resources around the globe interconnected through the Internet. At present, the term Internet is used to symbolize the following two situations:

- **Public Internet**, or just the Internet, that is not owned by any single entity – it consists of many independent TCP/IP networks that are tied together loosely. Initially, the public Internet was used to tie different university networks together. With time, several commercial and private networks have joined the public Internet. The computers on the public Internet have publicly known Internet Protocol (IP) addresses that are used to exchange information over the public Internet. The public Internet at present consists of thousands of networks.
- **Private internets**, or intranets, are the TCP/IP networks that are used by corporations for their own business, especially by exploiting Web technologies. Technically, an intranet uses the same technology as the public Internet – it is only smaller and privately owned and thus hopefully better

controlled and more secure. Thus, any applications and services that are available on the public Internet are also available on the intranets. This is an important point for the Web because many companies are using Web technologies on their intranets for internal applications (e.g., employee information systems).

**Extranets** are the TCP/IP networks that are owned by corporations to conduct business. These networks use the same Internet technologies; however, the physical network is collectivity owned by corporations to meet the security and reliability requirements imposed by the owners.

**Domain Naming Services (DNSs)** are used in the Internet to locate different resources. This protocol defines hierarchical naming structures that are much easier to remember than the IP addresses. For example, the machine with an IP address of 135.25.7.82 may have a domain name of shoeshop.com. A user “mills” may have an email address mills@shoeshop.com. The DNS naming structures define the organization type, organization name, etc. The last word in the domain name identifies an organization type or a country.

The Internet uses a large number of domain name servers that translate domain names to IP addresses (the IP routers only understand IP addresses). Domain names are used in the Internet as well as the Web. Figure 3-1 shows a conceptual and partial view of the Internet. This Internet shows three networks (a university network with two computers, a commercial company network, and a network in the UK). Each computer (“host”) on this network has an IP address and has been assigned a domain name as well. The Internet is very heterogeneous (i.e., different computers, different physical networks). However, to the users of this network, it provides a set of uniform TCP/IP services (TCP/IP hides many details). We will use this simple Internet to illustrate the key Internet capabilities.

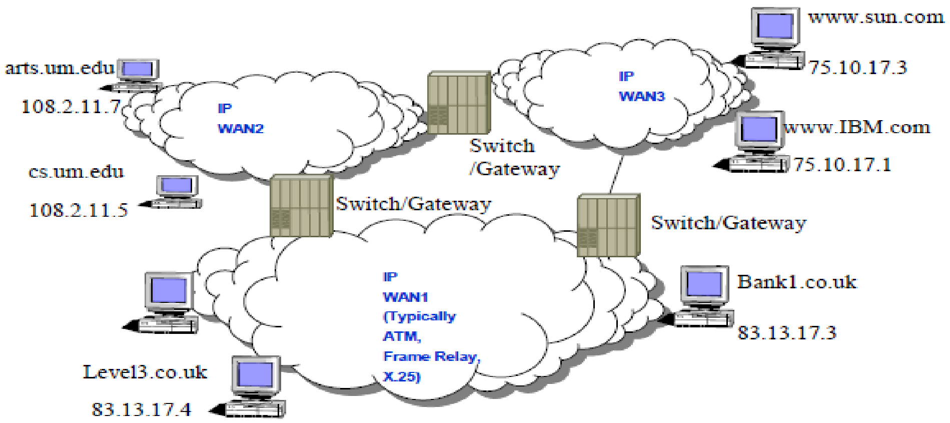
Since the Internet is based on TCP/IP, the applications and services provided by TCP are also available on the Internet. From an end-user point of view, the following services have been, and still are, used very heavily on the Internet:

- Email
- Telnet
- FTP
- Gopher

- WAIS (Wide Area Information Servers)

Electronic mail on the Internet is based on the **Simple Mail Transfer Protocol (SMTP)**.

This TCP-based protocol is the Internet electronic mail exchange mechanism. Email is still one of the most heavily used services in the Internet. Users on the Internet have email addresses such as johnm@cs.um.edu, hevner@sun.com and howard@bank1.co.uk.



•DNS (Domain Name Services) translates cs.um.edu to 108.2.11.5

•Telnet cs.um.edu = Telnet 108.2.11.5

•FTP cs.um.edu = FTP 108.2.11.5

**Figure 3-1: Partial View of Internet**

### 3.1.2 The Web at a Glance

The World Wide Web (WWW), commonly known as the Web, was started in 1989 by Tim Berners-Lee at the Geneva European Laboratory for Particle Physics (known as CERN, based on the laboratory's French name) [Berners-Lee 1999, 1993]. The initial proposal suggested development of a "hypertext system" to enable efficient and easy information-sharing among geographically separated teams of researchers in the High Energy Physics community. The initial proposal had three basic components:

- A common and consistent user interface Incorporation of a wide range of technologies and document types

- A “universal readership” to allow anyone sitting anywhere on the network, on a wide variety of computers, to easily read the same document as anyone else By the end of 1990, a line-browser (called www) was developed to implement the principles of hypertext access and the reading of different document types. In 1991, the line-browser was made available to the CERN community and a gateway for Wide Area Information Servers (WAIS) searches was developed. In 1992, a few more browsers were developed and around 50 websites (the machines that house Web documents) were implemented. During 1993, the Web took off – the number of websites increased to 500, the Web network traffic grew from 0.1 percent of Internet traffic to 1 percent (a 10-fold increase), and the Mosaic browser for X Windows was developed at NCSA (National Center for Supercomputing Applications at University of Illinois). Since 1994, the Web has been gaining popularity dramatically, with increases in the number of browsers, search engines, Web servers, and usage. The “First Generation of the Web,” is based on a few simple concepts and technologies. Due to the popularity of the Web, many limitations of the first generation started appearing. Based on this, a great deal of activity has focused on the “Next Generation of the Web,” Perhaps the best known activity from this work is XML and what is now being called “the semantic Web.”A good historical view of the WWW is presented by Tim Berners-Lee in his book “Weaving the Web” (Harper San Francisco, 1999).

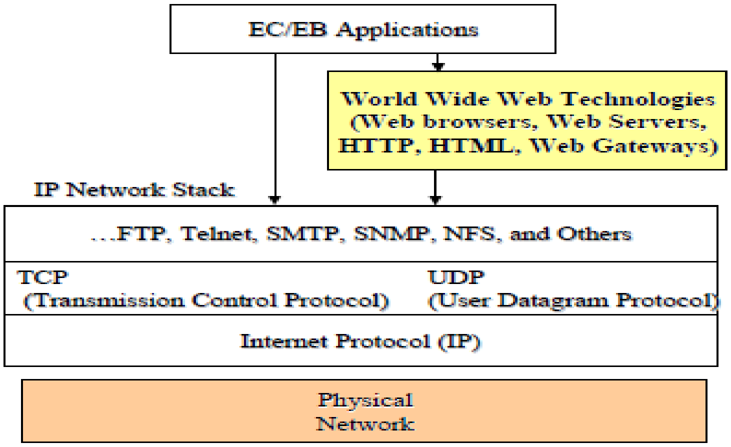

EC/EB Applications
World Wide Web Technologies (Web browsers, Web Servers, HTTP, HTML, Web Gateways)
IP Network Stack
...FTP, Telnet, SMTP, SNMP, NFS, and Others
TCP (Transmission Control Protocol)
UDP (User Datagram Protocol)
Internet Protocol (IP)
Physical Network

Figure 3-3: Technical View of World Wide Web

### 3.1.3 World Wide Web Technologies – The First Generation

Technically speaking, the Web is a collection of technologies that operates on top of the IP networks (i.e., the Internet). Figure 3.1.3 shows this layered view. The purpose of the WWW technologies is to support the growing number of users and applications ranging from entertainment to corporate information systems. Like many other (successful) Internet technologies, the first generation of the Web is based on a few simple concepts and technologies such as the following

- Web servers
- Web browsers
- Uniform Resource Locator (URL)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Markup Language (HTML)
- Web navigation and search tools
- Gateways to non-Web resources

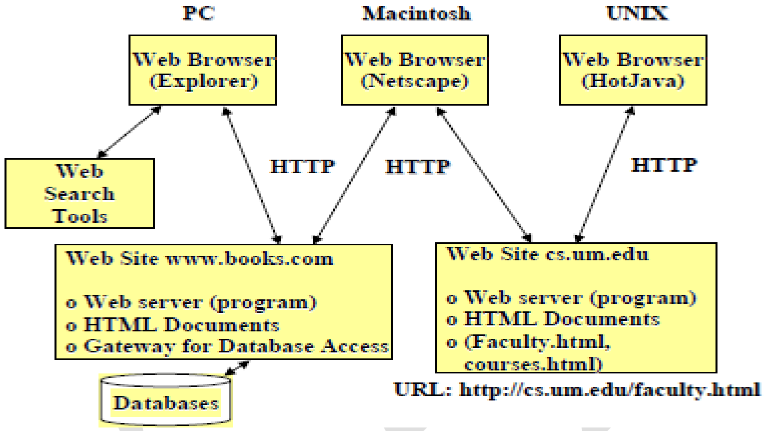


**Fig 3.1.4 Conceptual View of World Wide Web**

Let us briefly review these components and show how they tie in with each other through an example. We will discuss these components in more detail later in this chapter. ***Websites*** provide the content accessed by Web users. Websites are populated and in many cases managed by the content providers. For example, websites provide the commercial presence for each of the content providers doing business over the Internet. Conceptually, a website is a catalog of information for each content provider over the Web. In reality, a website consists of three types of components: a Web server (a program), content files ("Web pages") and/or gateways (programs that access non-Web content). A Web server is a program (technically a server process) that receives calls from Web clients and retrieves Web pages and/or receives information from gateways (we will discuss gateways later). Once again, a Web user views a website as a collection of files on a computer, usually a UNIX or Windows NT machine. In many cases, a machine is dedicated / designated as a website on which Web-accessible contents are stored. As a matter of convention in EC/EB, the entry point to a website is a “home page” which advertises a company business. Very much like storefront signs in a shopping mall, the home pages include a company logo, fancy artwork for attention, special deals, overviews, pointers to additional information, etc. The large number of websites containing a wide range of information to be navigated and searched transparently by Web users is the main strength of the Web. Figure 3.1.4 shows two websites – one for a shoe shop (www.shoes.com) and the other for a computer science department for a university (cs.um.edu).

***Web browsers*** are the clients that typically use graphical user interfaces to wander through the websites. The first GUI browser, Mosaic, was developed at the National Center for Supercomputer Applications at the University of Illinois. Mosaic ran on PC Windows, Macintosh, UNIX and Xterminals. At present, Web browsers are commercially available from Netscape, Microsoft and many other software/freeware providers. These Web browsers provide an intuitive view of information where hyperlinks (links to other text information) appear as underlined items or highlighted text/images. If a user points and clicks on the highlighted text/images, then the Web browser uses HTTP to fetch the requested document from an appropriate website. Web browsers are designed to display information prepared in a markup language, known as HTML. Three different browsers are shown in Figure 3-4. Even though these are different browsers residing on different machines, they all use the same protocol (HTTP) to communicate with the Web servers (HTTP compliance is a basic requirement for Web browsers). Most browsers at present are relatively dumb (i.e., they just pass user requests to Web servers and display the results). However, this is changing very quickly because of Java, a programming language developed by Sun Microsystems. Java programs, known as Java applets, can run on Java-compatible browsers. This is creating many interesting possibilities in which Java applets are downloaded to the Java-enabled browsers where they run, producing graphs/charts, invoking multimedia applications, and accessing remote databases. For a more detailed discussion of Java, see the tutorial on this topic in the Tutorial Module.

***Uniform Resource Locator (URL)*** is the basis for locating resources on the Web. A URL consists of a string of characters that uniquely identifies a resource. A user can connect to resources by typing the URL in a browser window or by clicking on a hyperlink that implicitly invokes a URL.

Perhaps the best way to explain URLs is through an example. Let us look at the URL "http://cs.um.edu/faculty.html" shown in Figure 3-4. The "http" in the URL tells the server that an HTTP request is being initiated (if you substitute "ftp" for "http," then an FTP session is initiated). The "cs.um.edu" is the name of the machine running the Web server (this is actually the domain name used by the Internet to locate machines on the Internet). The term "/faculty.html" is the name of a file on the machine cs.um.edu. The "html" suffix indicates that this is an HTML file. When this URL is clicked or typed, the browser initiates a connection to the "cs.um.edu" machine and initiates a "Get" request for the "faculty.html" file. Depending on the type of browser you are using, you can see these requests flying around in an appropriate window spot. Eventually, this document is fetched, transferred to the Web browser and displayed. You can access any information through the Web by issuing a URL (directly or indirectly). As we will see later, the Web search tools return a bunch of URLs in response to a search query. The general format of a URL is:

protocol://host:port/path

Where protocol represents the protocol to retrieve or send information. Examples of valid protocols are HTTP, FTP, Telnet, Gopher, and NNTP (Network News Transfer Protocol). Host is the computer host on which the resource resides port is an optional port number (this is not needed unless you want to override the HTTP default port, port 80) path is an identification, typically a file name, on the computer host.

***Hypertext Markup Language (HTML)*** is an easy-to-use language that tags the text files for display on Web browsers. HTML also helps in creation of hypertext links, usually called hyperlinks, which provide a path from one document to another. The hyperlinks contain URLs for the needed resources. The main purpose of HTML is to allow users to flip through Web documents in a manner similar to flipping through a book, magazine or a catalog. The website "cs.um.edu" shown in Figure 3-4 contains two HTML documents: "faculty.html" and "courses.html." HTML documents can imbed text, images, audio, and video.

***Hypertext Transfer Protocol (HTTP***) is an application-level protocol designed for Web users. It is intended for collaborative, distributed, hypermedia information systems. HTTP uses an extremely simple request/response model that establishes connection with the Web server specified in the URL, retrieves the needed document, and closes the connection. Once the document has been transferred to your Web browser, then the browser takes over. Keep in mind that every time you click on a hyperlink, you are initiating an HTTP session to transfer information stored in the two servers by using the HTTP protocol.

***Web navigation and search services*** are used to search and surf the vast resources available in "cyberspace." This term, as stated previously, was first introduced through a science-fiction book by Gibson [1984] but currently refers to the computer-mediated experiences for visualization, communication, and browser/decision support. The general search paradigm used is that each search service contains an index of information available on websites. This index is almost always created and updated by "spiders" that crawl around the websites chasing hyperlinks for different pieces of information. Search engines support keyword and/or subject-oriented browsing through the index. The result of this browsing is a "hit list" of hyperlinks (URLs) that the user can click on to access the needed information. For example, the Web users in Figure 3-4 can issue a keyword search, say by using a search service for shoe stores in Chicago. This will return a hit list of potential shoe stores that are Web content providers. You, then, point and click until you find a shoe store of your choice. Many search services are currently available on the Web. Examples are Yahoo, Lycos and Alta Vista. At present, many of these tools are being integrated with Web pages and Web browsers. For example, the Netscape browser automatically invokes the Netscape home page that displays search tools that you can invoke by just pointing and clicking. It is beyond the scope of this book to describe the various Web navigation and search tools. Many books on the Internet describe these search tools quite well. For example, the book by December [1995] has an extensive discussion of Web search and navigation tools with information about how to locate and use them.

***Gateways to non-Web resources*** are used to bridge the gap between Web browsers and the corporate applications and databases. Web gateways are used for accessing information from heterogeneous data sources (e.g., relational databases, indexed files and legacy information sources) and can be used to handle almost anything that is not designed with an HTML interface. The basic issue is that the Web browsers can display HTML information. These gateways are used to access non-HTML information and convert it to HTML format for display on a Web browser. The gateway programs typically run on websites and are invoked by the Web servers. At present, Common Gateway Interface (CGI) is used frequently. We will discuss CGI gateways and other types of Web gateways later in this chapter. “Relational gateways” that provide access to relational databases from Web browsers are an area of active work.

### 3.2 How does Wireless Web Really Work?– A Simple Wired Access Example

Before discussing wireless access to the Web, let us first consider an example of wired Web access to show the interrelationships between the main components discussed so far. Figure 3-2. illustrates how the Web components can be used for purchasing from a department store, “clothes.com.” This store wants to advertise its products on the Web, (i.e., wants to be a Web content provider). The store first designates a machine, or buys services on a machine, called “clothes.com” as a website. It then creates an overview document, “overview.html,” that tells the potential customers of the product highlights (think of this as the first few pages of a catalog). In addition, several HTML documents on the website for different types of clothes (men.html, women. html, kids.html) are created with pictures of clothes, size information, etc. (once again think of this as a catalog). We can assume that the overview page has hyperlinks to the other documents (as a matter of fact, it could have hyperlinks to other branches of clothes.com). In reality, design of the Web pages would require a richer, deeper tree structure design as well as sequential links for alphabetical and keyword searches needed to support the “flipping through the catalog” behavior.

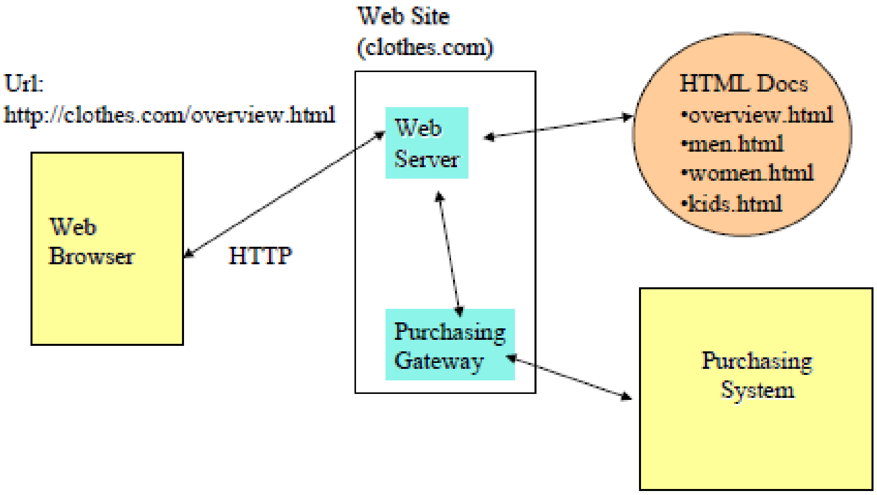
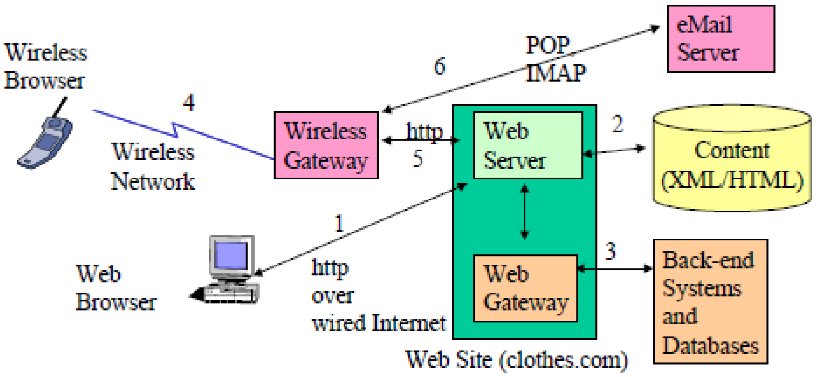


**Figure 3-2.1 Conceptual View of an Internet-based Purchasing System**

Once HTML documents have been created on the Web server, an Internet user can browse through them as if he/she is flipping through a catalog. By using the browser, the Internet user establishes an HTTP session with the website – the entire Internet machinery discussed above (IP addresses, routers, etc) is used to establish this connection. To make the connection, the customers of clothes.com typically supply the URL, directly or indirectly, for the overview (http://clothes.com/overview.html) and then use the hyperlinks to look at different types of clothes. Experienced customers may go directly to the type of clothes needed (e.g., men may directly go to the "men.html" document). As shown in Figure 3-5, the URL consists of three components: the protocol (http), the Web server name (clothes.com), and the needed document (overview.html). HTTP provides the transfer of information between the Web users (the clients) and the Web Servers. At first, clothes.com is only using the Web to store an electronic catalog. After a customer has browsed through the catalog and has selected an item, he/she calls the store and places an order. Let us say that clothes.com also wants the customers to purchase the items over the Internet. In this case, a "Purchasing Gateway" software is developed and installed at the website. This gateway program gets into action when a user clicks on the "purchase" button on his screen. It prompts the user with a form (HTML supports forms) that the user fills out. The gateway program uses this form information to interact with a purchasing system that processes the purchase (see Figure 3-5). The purchasing system can be an existing system that is used for traditional purchasing. The role of the gateway is to provide a Web interface to the purchasing system.

**A Simple Wireless Web Example**

Figure 3-1 expands and generalizes the example discussed above to include wireless access. Steps 1, 2, and 3 show how Web content is accessed and a back-end system (such as purchasing) is invoked from regular Web browsers. We have discussed these steps previously. The difference is that now the same activities (accessing clothes.com and purchasing goods) are being performed from cellular phones by using steps 4 and 5. In addition, email services are also being invoked from the same cellular phone by using step 6. Let us go through some details of these additional steps. Steps 4 and 5 entail connection to the clothes.com site through a wireless gateway. The main purpose of this gateway is to convert the wireless network request (step 4) into a regular HTTP request (step 5) so that the web server does not know if the request originated from a cellular phone or a desktop web browser. This has a major advantage that the same Web content and mechanisms to invoke back-end systems can be re-used without any changes. The wireless gateway also does the reverse processing on outbound traffic – it converts regular web content to a format that can be displayed on the cellular phone. An example of a wireless gateway is the WAP (Wireless Application Protocol) Gateway, commercially available from companies such as Nokia. We will take a closer look at wireless gateways later in this chapter and next chapter. Step 7 shows how email can be accessed from the same cellular phone. In this case, the wireless gateway detects that the content is not on a Web server; instead it is on an email server. Consequently, it establishes an email session by using POP (Post Office Protocol) or some other email protocol and converts the content back and forth between the email server and the cellular phone.



1. Access from Web browser to Web Server over wired Internet
2. Access Web contents from HTML/XML files
3. Access to non-Web content through a Web gateway
4. Access from cellular phone over a wireless network
5. Access from wireless gateway to Web Server over wired Internet
6. Access from the Wireless Gateway to an email server

**Conceptual View of Wireless Access to Web and Email**

The main message should be clear – wireless gateways play a key role in interconnecting the mobile devices to existing resources (Web content, online purchasing facilities, email services). The level of translation performed by the wireless gateway depends on the differences between the front-end (wireless) and back-end (wired) systems. For example, if the wireless network is an 802.11 LAN that already supports IP, then the translation is minimal. But if the wireless network is a 1G analog cellular system, then heaven help you!

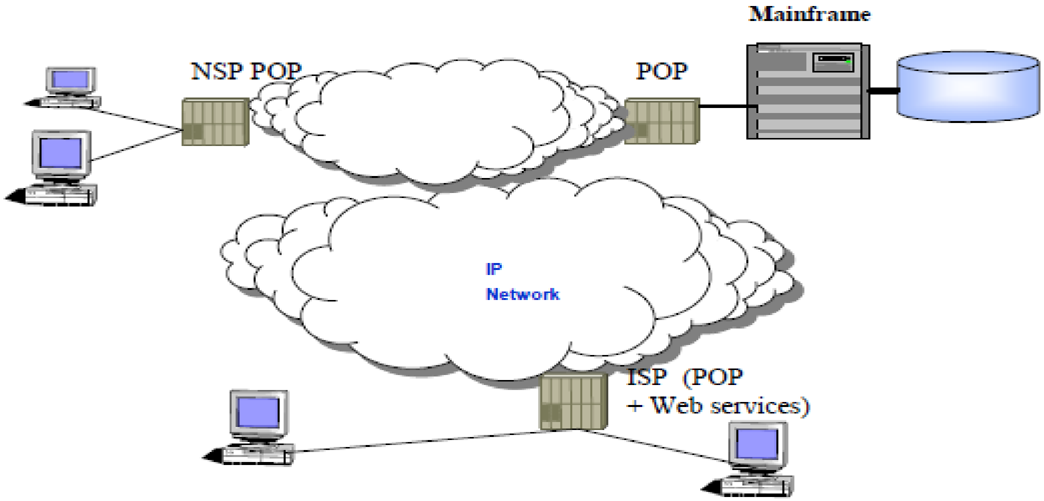
## 3.3 Mobile IP – Supporting Mobile Devices over the Internet

### 3.3.1 Overview

Mobile IP was developed so that mobile devices (PDAs, portable computers) could maintain Internet connectivity while moving from one Internet attachment point to another. Consider, for example, that you are in your office with your laptop that is connected to the Internet. Assume that you issued a database query but then detached your laptop, went to a meeting room, and reconnected your laptop in the meeting room. In this case, Mobile IP will allow the system to recognize that you have moved and will send the results from your query to your new location (the meeting room). The main idea of Mobile IP is that the same Internet connection address is maintained as you move your mobile device from one location to another. As we will see, the traffic is forwarded by using a “care of” address. At this point, it is best to differentiate between a mobile and nomadic user:

- Mobile – user’s point of attachment changes dynamically and all connections are automatically maintained despite the change.
- Nomadic – user’s Internet connection is terminated each time the user moves and a new connection is initiated when the user dials back in. A new, temporary IP address is assigned. Let us briefly consider how IP addresses are assigned before getting into Mobile IP. Basically, Network Service Providers (NSPs), also known as Internet Access Providers (IAPs), are the organizations that provide the physical network, i.e., give you a communication line and an access port on the Internet. You can think of IAPs as the local authorities that provide you with roads and signs to get you to the shopping malls. For dial-up users, an NSP provides a bunch of POPs (points of presence). that the users can dial into as a local call. An example of NSP is UUNET, which has POPs around the globe. I am a regular user of UUNET. A GUI shows me the phone number of the nearest POP (I just type in the name and country of the city). When I travel, I quickly locate a UUNET number and make a local call to reach my office computers. Internet service providers (ISPs) go beyond the network pipe and offer Internet services such as email, Web hosting and Web

surfing. An ISP may rent NSP, i.e., use an existing POP, or own a network and thus may own POPs. Examples of ISPs are America Online and Asia Online. Figure 3.3.1 shows how a computer is connected to an ISP Server through an NSP. Let us quickly review routing in the Internet (IP routing) before discussing the logistics of Mobile IP.



•POP (Point of Presence) provided by an NSP only provides a local phone access. The user can choose an ISP

•An ISP provides an IP address (user dials in)

•When the user moves, has to disconnect and redial.

**Figure 3.3.1: A Traditional Internet Connection**

**Internet Routing – A Quick Tour**

The Internet consists of several IP-based physical networks (#a network of networks) that are interconnected together. An example of an Internet (IP network) is shown in Figure 3.1.4. This IP network connects many disparate physical networks into a coordinated unit and hides the details of the physical network hardware; it allows computers to communicate independent of their physical network connections

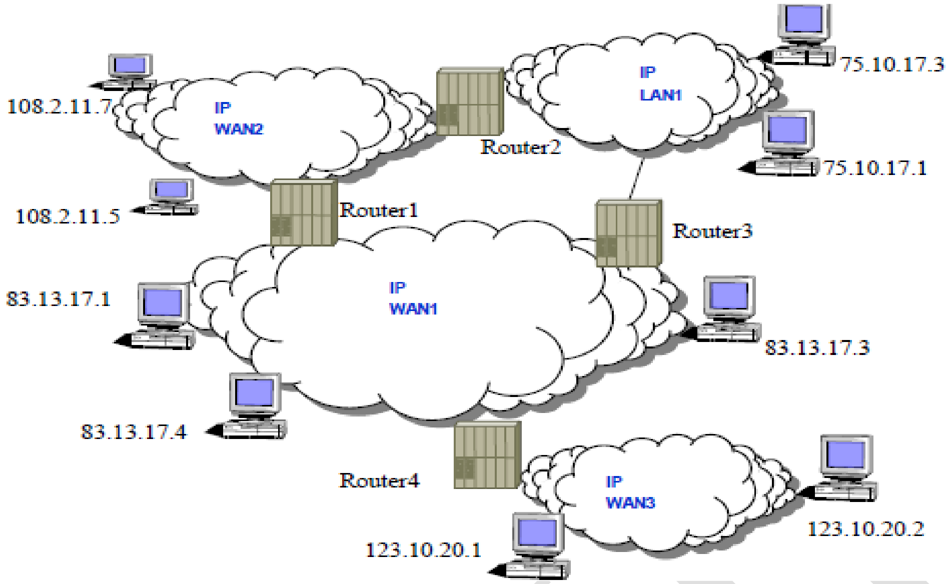


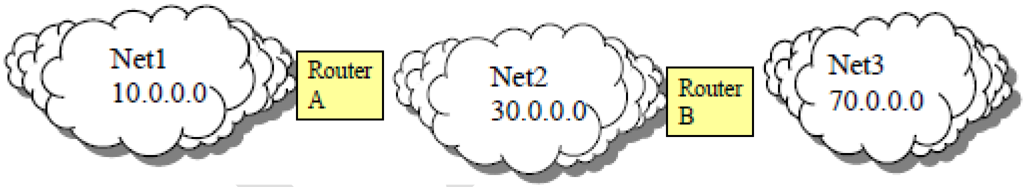
**Figure** 3.1.4. **A Sample IP Network**

Internet ***routers***, sometime also referred to as Internet gateways, are used between physical networks of an IP network and perform the functions of a relay that directs traffic to its destination. Routers are software programs, typically residing in dedicated computers that shuffle messages between physical networks. For example, the routers shown in Figure 3-14 pass the messages between the four networks. In general, an outgoing message from a host first checks to see if its destination is on the same physical network. If its destination is not on the physical network, then it goes to a router for routing. The role of a router becomes more complex as the complexity of the IP network grows. In a complex network, the routers must understand the network topology and must know how to get to the next router. For example, Router4 in Figure 3.1.4 must know how to pass messages from WAN3 to LAN1 through the intermediate routers. In all cases, routers are responsible for routing messages to a destination network and not to a destination host. In most cases, routers are dedicated computers that house the routing tables. The size of the routing table depends on the number of physical networks and not on the number of computers in an Internet.

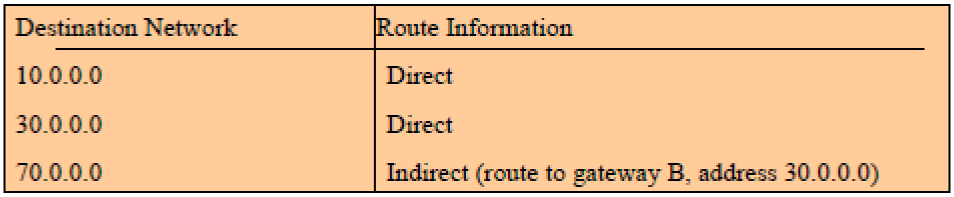
Every host and router in the Internet has an IP address, which encodes its network number and host number. The Internet address is a 32-bit address commonly denoted as four decimal numbers separated by periods, e.g., 125.102.112.5. The IP address is unique: no two machines have the same IP address. If an enterprise cannot present globally unique addresses to the Internet, The IP sends each message as a ***datagram*** which is its basic unit of information transfer. Each datagram contains a header and data areas. The datagram header contains the IP addresses of the sender and receiver. The datagrams are routed through the Internet by using a variety of routing algorithms. The choice of the routing algorithm depends on the nature and complexity of the Internet. The IP routing occurs at a higher level (global) than the physical network routing in a subnet. The IP routing is responsible for transferring messages between the physical networks of an Internet. The physical networks (subnets) are interconnected through gateways. The routing of a message within a physical network (e.g., an Ethernet) is the responsibility of the network routing (the data link protocol) mechanism of the network.

The route can be direct (within a physical network) or indirect (between networks through gateways). Internet routing algorithms usually employ routing tables which show possible destinations. An example of a routing table for a simple internet is given in Figure 3.1.5. A typical routing algorithm used in IP is as follows:

- Extract the destination address DA from the datagram.
- Find the route for DA from the routing table.
- If DA is a direct path (within this subnet), send the message directly.
- If DA is an indirect path, send the message to the proper subnet or gateway.
- If none, then give a routing error.



a) A Simple IP Network



| Destination Network | Route Information |
|---|---|
| 10.0.0.0 | Direct |
| 30.0.0.0 | Direct |
| 70.0.0.0 | Indirect (route to gateway B, address 30.0.0.0) |

b) Routing Table for Router A

**Figure 3.1.5: Example of a Routing Table**

Briefly, the Internet datagrams travel from router to router until they reach a router that can deliver them directly to the destination host. If a router cannot route or deliver a datagram due to an addressing problem or congestion, it needs to instruct the host to take action. The mechanism commonly employed to communicate the errors is the ***Internet Control Messages***

***Protocol (ICMP).*** ICMP messages travel across the Internet in the data portion of the datagram just like all other traffic. The destination of an ICMP message is the IP software on the destination machine and not the application process. Basically, ICMP provides a communication mechanism between the IP software at various machines (hosts and/or gateways) in the networks. ICMP is considered a required part of IP. More details about

ICMP can be found in the DARPA standard RFC 792.

**How Does Mobile IP Work?**

Now let us see how the dynamic addressing will work in a mobile IP environment by using Figure 3.1.6. Let us assume that a mobile computer C1 is assigned to a particular network, called the ***home network*** for C1. The IP address on the home network is static and is called the ***home address***. for C1. Now, let us assume that the mobile computer has moved to another network, known as a ***foreign network***. To be operational, C1 first registers with a network node on the foreign network. This node is called a ***foreign agent.*** The foreign agent takes responsibility of C1 and gives its address as a ***"care-of address"*** to the agent on the home network, called the ***home agent.*** As illustrated in Figure 3-16, the home agent gets all the incoming traffic for C1 (step 1), the traffic is routed it to the "care-of" address – the foreign agent (step 2), the foreign agent routes the traffic to C1 in the foreign network (step 3), and the return traffic is routed back to the IP server without having to go through the home agent (steps 4 and 5)

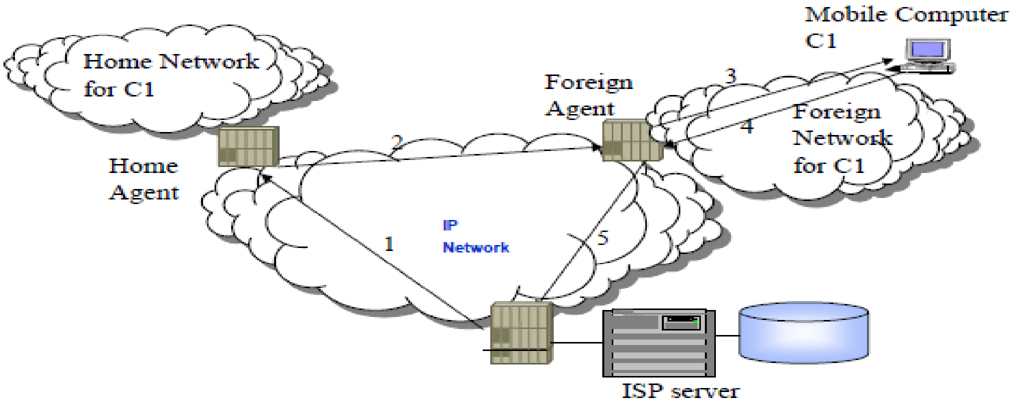


Figure 3-16: A Mobile IP Scenario

## Capabilities of Mobile IP

Mobile IP includes three basic capabilities to support the operations shown in Figure3-16.

- Discovery: A mobile node uses a discovery procedure to identify prospective home and foreign agents.
- Registration: A mobile node uses an authenticated registration procedure to inform the home agent of its care-of address.
- Tunneling: Tunneling is used to forward IP datagrams from a home address to a care-of address.

These capabilities are reviewed briefly.

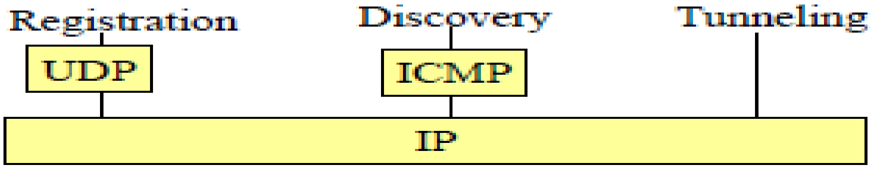


**Figure 3-17: Mobile IP Processes**

## Discovery

A mobile node is responsible for an ongoing discovery process because it must determine if it is attached to its home network or a foreign network. The transition from the home network to a foreign network can occur at any time without notification to the network layer. A router planning to act as a foreign agent issues agent advertisement messages periodically (i.e., “I want to be your agent, do you want my services?”). The mobile node listens for agent advertisement messages and compares the network portion of the router’s (foreign agent’s) IP address with the network portion of its home address. If there is a match, then the mobile node knows that it is on a foreign network and that this router can act as a foreign agent.

Foreign agents are expected to issue agent advertisement messages periodically. However, if a mobile node needs agent information immediately, it can issue ICMP router solicitation messages explicitly. Any agent receiving this message will then issue an agent advertisement.

Thus a mobile agent can explicitly ask for a foreign agent. A mobile node may move from one network to another due to some handoff mechanism without the IP level being aware.

The agent discovery process is intended to enable the agent to detect such a move.

As a result of the discovery process, as stated previously, the foreign agent gives its IP address as a "care-of address" so that the home agent can route the traffic to the "care-of" address.

The foreign agent then routes the traffic to the mobile node in the foreign network. If the mobile node moves to a network that has no foreign agents, or all foreign agents are busy, it can act as its own foreign agent.

**Registration Process**

After a mobile node finds a suitable foreign agent, it sends a registration request to the foreign agent requesting forwarding service. The foreign agent relays this registration request to the home agent. The home agent accepts or denies the request and sends a registration reply to the foreign agent, which in turn relays a reply to the mobile node.

**Registration procedure security** is a major problem. Mobile IP is designed to resist the following types of attacks:

- A node pretending to be a foreign agent sends registration request to a home agent to divert mobile node traffic to itself.
- An agent replays old registration messages to cut the mobile node from the network. The techniques used to protect against these two attacks consist of message authentication, among others. For message authentication, the registration request and reply contain an authentication extension. Types of authentication extensions include:
- Mobile-home – provides for authentication of registration messages between mobile node and home agent; must be present.
- Mobile-foreign – may be present when a security association exists between mobile node and foreign agent.

- Foreign-home – may be present when a security association exists between foreign agent and home agent.

**Tunneling**

The home agent intercepts IP datagrams sent to the mobile node's home address. The home agent informs other nodes on the home network that datagrams to the mobile node should be delivered to the home agent. The datagrams are now forwarded to the care-of address via ***tunneling.*** Basically, tunneling means that a datagram is encapsulated in an outer IP datagram. Mobile IP encapsulation options (assuming knowledge of IP addressing) are:

- IP-within-IP – entire IP datagram becomes payload in new IP datagram. Original, inner IP header basically is unchanged. Outer header is a full IP header.
- Minimal encapsulation – new header is inserted between original IP header and original IP payload. Original IP header is modified to form new outer IP header.
- Generic routing encapsulation (GRE) – developed prior to development of Mobile IP.

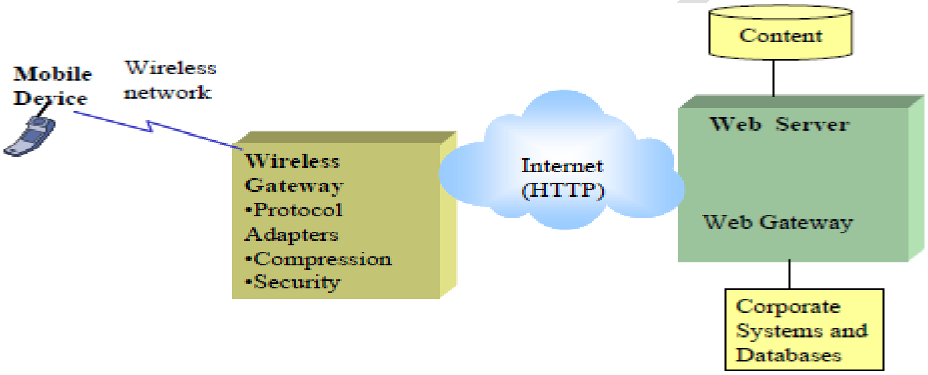
**3.4 World Wide Web for Wireless – A Closer Look**

**3.4.1 Accessing the Web from Mobile Devices and the Wireless Gateways**

Wireless gateway is the bridge between two distinct worlds: the Internet model and the wireless phone/data network model. The wireless gateway shown in Figure 3.4.1 translates between the Web server and the mobile devices. The wireless gateway, a software module, supports a thin client model by allowing the handset to be simple and inexpensive. For example, this gateway can take over directory processing, data conversions, fraud management, and network provisioning. The gateway thus offloads these computing tasks from the handset. The gateway typically includes the following functionality:

- Protocol Adapters – the protocol adapters translate requests from the wireless network to the Web protocol stack.
- Content Encoders and Decoders – the content encoders translate Web content into compact encoded formats to reduce the size and number of packets traveling over the wireless data network. This architecture ensures that mobile terminal users can browse a variety of Web content and

applications regardless of the wireless network they use. The content and applications are hosted on standard Web servers and can be developed using Web technologies such as CGI scripting, servlets, and Java Server Pages. Several wireless gateways, such as WAP Gateways, are commercially available at present. We will look at WAP in the next chapter. Although mobile devices can access Web content by using the traditional Web technologies, XML and the Semantic Web are playing an increasingly important role in future wireless web scenario. The next section introduces these technologies briefly.



**3.4.1 Wireless Gateway**

### 3.4.2 Semantic Web and its Role in Mobile Web Access

The first-generation Web, needless to say, gained popularity due to its simplicity and ease of use. However, the use of this technology has spread far beyond the initial design goals and imagination of the designers. Thus, some limitations of the initial Web technologies have started to show. In particular, the following limitations are worth noting for mobile computing:

- Desktop display-oriented. The original Web browser assumed a desktop display. However, mobile computing users want to access and display Web information on Palm Pilots, cellular phones, and other mobile devices.
- Technical limitations. The first-generation Web suffers from many technical problems. For example, the technology for Web gateways (CGI – Common Gateway Interface) does not scale well (i.e., is not suitable for a hundred or more users simultaneously). In addition, the original HTTP is stateless (i.e., every time you access a Web page over HTTP, it has no memory of what did you access before).
- Suited for human viewing only. The HTML documents can be only used for displays. However, in some cases, the consumer is not a human. For example, if you send an HTML document to a

device, then the device has to “screen scrape” all the tags to get useful data. This is a major problem in mobile applications because many mobile devices may need to understand the HTML documents.

The WWW Consortium (known as W3C) has embarked on work in several directions to overcome these and other possible limitations. This work, under the general umbrella of Semantic Web (also known as Next Generation Web), includes the following key developments (see Figure 3-19):

- XML (Extended Markup Language) – a family of standards and services introduced to improve machine-to-machine communications. We will study XML in Section 3.6.3.
- Variations of markup languages such as WML (Wireless Markup Language), MathML, SVGML, SMIL, etc. for different applications.
- Improvements in the core technologies such as HTTP, and also introduction of more choices for Web gateways.
- Web automation efforts that introduce an object model for the Web. These efforts include DOM, RDF, PICS, P3P and others.

PICS: Platform for Internet Content Specification

P3P: Platform for Privacy Preferences

SMIL: Synchronous Multimedia Interaction Language

DOM: Document Object Model

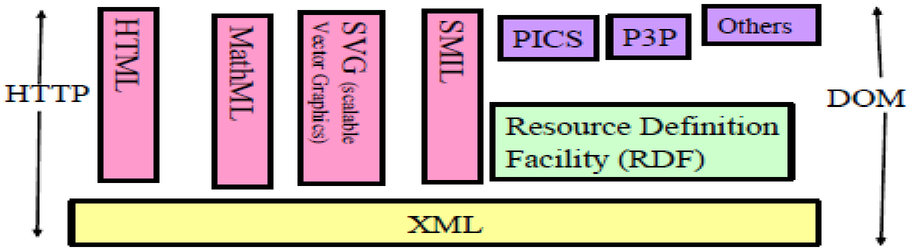
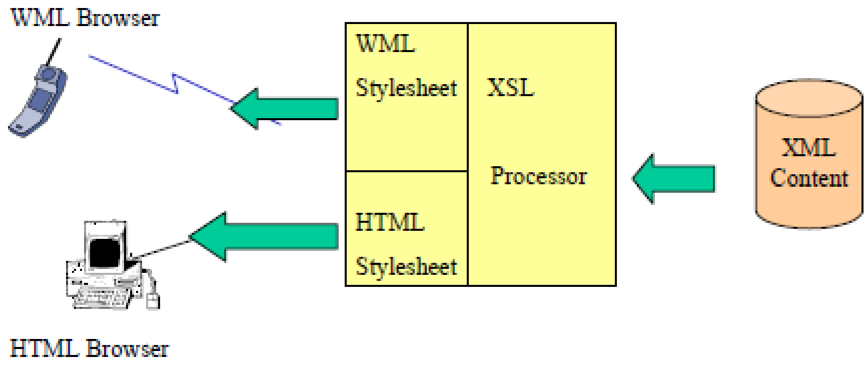

HTTP
HTML
MathML
SVG (scalable Vector Graphics)
SMIL
PICS
P3P
Others
Resource Definition Facility (RDF)
DOM
XML

**Figure 3-19: Next Generation Web**

It can be seen from Figure 3-19 that XML is at the core of the Next Generation Web. XML is also playing a key role in the future of the Wireless Web as shown in Figure 3-20. For example, WML is an XML-based language – thus it is an easy markup language for existing Web developers to learn. In addition, content written in XML-defined markup languages can be automatically translated into content suitable for either HTML or WML by using an XSL style sheet (see Figure 3-20). Basically, content written in well-formed XML can also be translated to other XML-based markup languages such as Voice XML, using a different XSL style sheet.



**3.20 The Future of Content Description**

### 3.5 Mobile Web Services

Accessing WS from mobile devices is a major area of work at present. For example, Microsoft has developed a Mobile Internet Toolkit (MMIT) that supports development of mobile computing applications based on WS by using the Microsoft .NET Framework (see next chapter). But MMIT is a proprietary technology. Mobile Web Services (MWS) is a new open specification that extends the core Web Services specifications to include the special capabilities and requirements of mobile computing. A framework for Mobile Web Services has been proposed to enable new services and products to be created for mobile computing.

MWS is evolving at the time of this writing. The following have been identified:

- Application of WS-Security to mobile network security services. For example, a GSMstyle SIM security device has been accepted for authentication.
- Development of a set of payment mechanisms within the Web Services architecture
- SMS services and MMS services
- Location-based services

Other areas for work within the activity have also been identified and are under review at the time of this writing. The two main areas of work are optimal transmission of WS requests over slow cellular networks and efficient processing of WS by mobile devices with processor limitations.

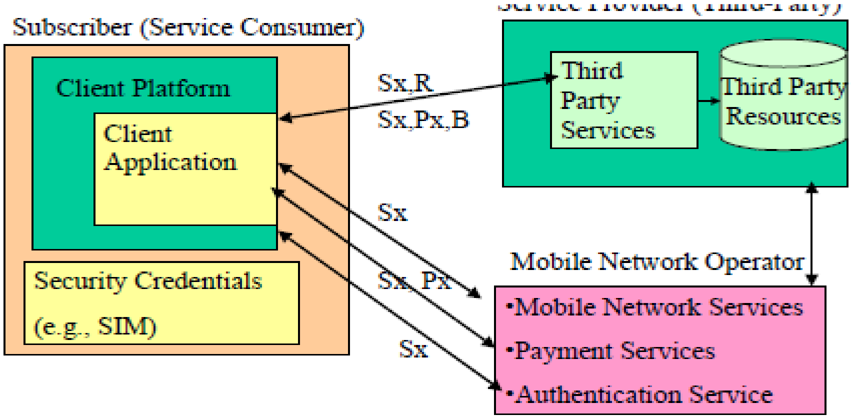


**Figure 3-27: Mobile Web Services**

Figure 3-27 shows a conceptual view of the initially proposed three principal components of MWS and the interactions among them. The Subscriber is a service consumer (a client) that needs services of a Third-Party Service Provider (SP). One or more Client Applications are used by the subscriber – these applications run under the control of a Client Platform (e.g., a Symbian operating system) and use Security Credentials such as a SIM card. The SP offers a set of services that are defined through WSDL and possibly stored in a UDDI. For example, a bank could be an SP that provides account review, bill payment, and fund transfer as three possible services that have been defined through WSDL. A Mobile Network Operator is the third player in MWS – it provides authentication and payment services in addition to its own services, known as Mobile Network Services. These Mobile Network Services are Web

Services and represent SMS, MMS, Location or other proprietary services. The Authentication Service and the Payment Service are also Web Services operated by the Mobile Network Operator to perform authentication and payment authorization, respectively.

The subscriber has a business relationship with a Mobile Network Operator and subscribes to one or more of the Operator services (e.g., SMS).

### 3.6 Mobile Computing Platforms, Middleware, and Servers

Other mobile or fixed devices to support mobile computing applications. Platforms to support these applications, called ***mobile computing platforms***, provide interconnectivity services between partners and transfer information in a secure and efficient manner. These platforms, the focus of this chapter, enable the operation and, in many cases, development and deployment, of mobile computing applications such as mobile messaging, mobile ommerce, mobile business, and many others discussed in Chapter 2. Figure 3.5.1 illustrates the position of mobile computing platforms relative to the mobile applications and physical wireless networks, and serves as a general framework for our discussion. As depicted in Figure 3.5.1, these platforms provide three types of services:

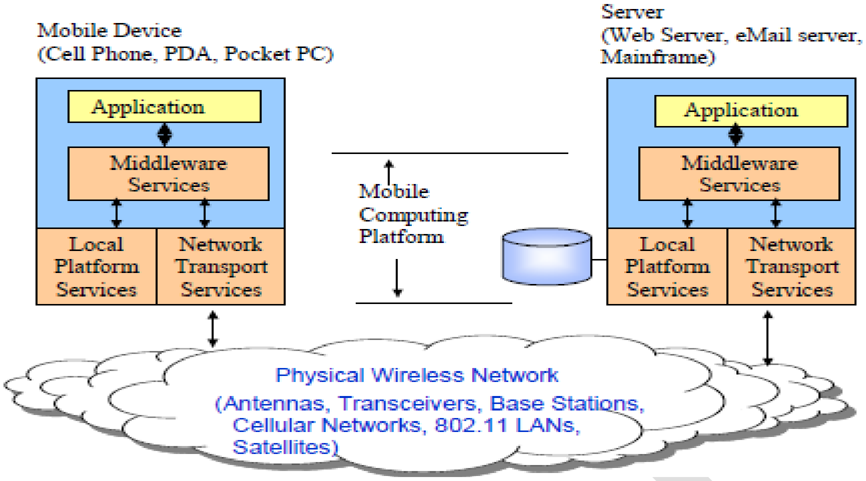

Mobile Device
(Cell Phone, PDA, Pocket PC)
Server
(Web Server, eMail server, Mainframe)
Application
Middleware Services
Local Platform Services
Network Transport Services
Application
Middleware Services
Local Platform Services
Network Transport Services
Mobile Computing Platform
Physical Wireless Network
(Antennas, Transceivers, Base Stations, Cellular Networks, 802.11 LANs, Satellites)

**Figure** 3.5.1**: Platforms for Mobile Applications**

Mobile computing platforms support the development as well as operation of mobile applications such as mobile messaging, mobile commerce, mobile e-business, and others.

- Mobile computing platforms consist of the following:
- Local platform services that run on the mobile device (clients) and also on the servers

- Interconnectivity software (the wireless middleware) that interconnects the two
- Network transport services that transfer message over the wireless networks
- Wireless middleware itself can be subdivided into:
- Individual services such as compression and content conversion
- Wireless gateways that combine many individual services together to provide run-time support
- Mobile application servers that go beyond the gateways and include mobile application development, monitoring, and control features.
- Local services support the individual mobile devices. These services consist of operating systems, database managers, transaction managers, and utilities for mobile devices.

- Middleware services interconnect mobile users, databases and applications with each other. Mobile computing applications need this middleware to smooth over the mobile computing issues as much as possible, so that the same applications can run on wired as well as wireless networks.
- WAP (Wireless Application Protocol) is an open specification for mobile computing platforms. It supports a WAE (Wireless Application Environment) and uses WML (Wireless Markup Language).
- i-mode, developed by NTT DoCoMo, is a popular mobile computing platform in Japan and is currently gaining momentum in the US. It uses special phones capable of voice and packet transmission along with a browser installed. I-mode phones are specialized phones, with larger windows for multimedia, that display content in cHTML (compressed HTML) over packet-switching networks.
- Wireless Java is the general umbrella name under which Sun is supporting its Java platform for developing wireless applications. Java 2 Micro Edition (J2ME) is the core technology in wireless Java for writing applications that run on small hand-held devices.
- The Microsoft Mobile Internet Toolkit (MMIT) is an extension of the Microsoft .NET framework for building Wireless applications. MMIT has two interesting features: it automatically generates code (WML, cHTML, and HTML) for different types of mobile devices, and it is built around .NET and Visual Studio – popular platforms for application development at present.
- BREW, from QualComm, provides application developers with a platform in which to develop their products, and to incorporate the same features as J2ME, including crossdevice platform capabilities. BREW currently uses Microsoft .NET Visual Studio.
- VoiceXML is a markup language for voice browsers. It is designed for creating audio dialogs that feature synthesized speech, digitized audio, and recognition of spoken and digitized voice mail.
- Specialized platforms for systems such as wireless sensor networks are evolving.

### 3.6 Wireless Middleware

What is Wireless Middleware?

Simply stated, wireless middleware interconnects mobile users, databases and applications across wireless networks. Wireless middleware, also known as mobile computing middleware, is a special class of general purpose middleware (see the sidebar, "What is Middleware?") that smoothes over the mobile computing issues, as much as possible, so that the same applications can run on wired as well as wireless networks. The following common features of wireless middleware products are needed to support mobile computing applications [Umar 2004, Vichr 2001]:

- **Connection and message delivery**: Middleware helps establish connections between mobile clients and servers over wireless networks and delivers messages over the connection. It also stores and forwards messages if the user is disconnected from the network.
- **Transformation**: The middleware transforms data from one format to another (e.g., HTML to WML). The transformation may be intelligent enough to transform different types of data to different types of devices. For example, it can produce VXML or WML depending on the type of device.
- **Detection and storage**: Wireless middleware products can detect and store mobile device characteristics in a database. Upon detecting the type of mobile device or channel being used (e.g., GSM or 802.11 frequency range), the middleware can optimize the wireless data output according to device attributes.
- **Optimization**: Middleware products can compress data to minimize the amount of data being sent over a slow cellular wireless link.
- **Security**: Security features can be imbedded in wireless middleware to ensure end-to-end security. For example, digital certificates for handheld devices can be managed by a middleware service.
- **Operation support**: Middleware can offer network and systems management utilities and tools to allow monitoring and troubleshooting wireless devices and networks. A variety of general-purpose middleware services have emerged over the years. Example are CORBA, DCOM, MOMs (message-oriented middleware), and others.

Many of these have been extended and specialized for wireless. For example, Wireless
CORBA was specified by OMG as a specialization of CORBA. In the same vein, Sun's J2ME (Java 2 Micro Edition) has been specified as a family member of the Sun J2 EE (Java 2 Micro Edition)

product line. In addition, common message-oriented middleware (MOM) has been extended for wireless situations  Naturally not all these features are needed for every mobile computing application. It is thus important to review the characteristics of mobile computing environments that are unique and then discuss the categories of applications that place different demands on the underlying network and middleware.

Wireless Gateways and Mobile Application Servers service (e.g., connectivity, security, compression), these services are being packaged together as:

- Wireless gateways that combine many individual services together to provide *run-time* support.
- Mobile application servers that go beyond the gateways and include mobile application *development and deployment* features. Although this packaging does not work perfectly in all situations, it provides a conceptual framework for discussing and categorizing the wide range of products that are becoming available to support mobile computing.

What is a Wireless Gateway?

Simply stated, a gateway is a converter – it converts contents and protocols for disparate parties to talk to each other. Wireless gateways package several wireless middleware services that perform conversions between two distinct worlds: the Internet world and the wireless phone/data network world. The wireless gateway shown in Figure 4-18 translates between the Web server and the mobile devices and uses a three-tiered approach for mobile computing applications. The gateway is the middle tier that contains many middleware services and thus supports a thin client model by allowing the handset to be simple and inexpensive. As a establishment of sessions between client processes and server processes, security, compression/decompression, and failure handling. Specifically, a wireless gateway offers some of the following services:

- Connectivity services that allow the remote partners on a network to locate each other (through a directory or naming service, typically), open a connection with the remote partner, and transfer information between the remote partners
- Protocol adapters that translate requests from the wireless network protocols to the Web protocol stack
- Content encoders and decoders that translate Web content into compact encoded formats to reduce the size and number of packets traveling over the wireless data network

- Directory, naming, and location services for remote partners
- Security services such as identification, authentication, confidentiality, authorization and access control
- Performance enhancements (such as caching and compression)

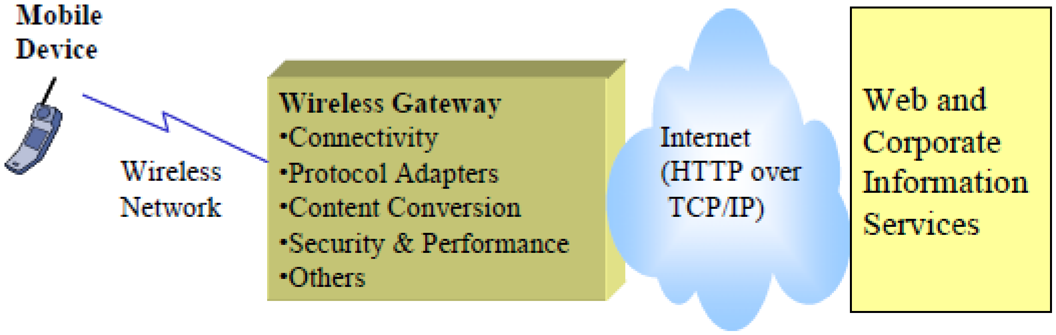


**Figure 3.6.1 Wireless Gateway**

The main advantage of a wireless gateway is that a vendor provides an integrated set of commonly used services. The services provided by the gateway depend on the differences between the two sides of the wireless gateway. For example, if the wireless network side is 802.11 LAN supporting laptops, then the gateway may not need to provide hardly any functionality because TCP/IP runs on both sides and the laptops can handle normal Web interactions with HTML over HTTP. But if the wireless side is a 1G cellular network with handsets, then many different types of conversions are needed by the wireless gateway. An example of a wireless gateway is the iBus MOM server that performs many conversions.

Other examples of wireless gateways are the WAP Gateway from Motorola, the i-mode gateway from DoCoMo, and the VoiceXML gateway from IBM. In general, XML and its variants are playing an increasingly important role in the future of wireless gateways.

What is a Mobile Application Server?

The growing demand for wireless applications dictates that the mobile applications must be developed quickly and be scalable, secure, robust, and flexible. This has several implications:

- Quick deployment means that an integrated development environment (IDE) is needed.
- Scalability means that a mobile application may be used by thousands or even millions of users.
- Security means authentication of users, confidentiality, non-repudiation of transactions, etc.

🗞 Robustness implies that a transaction issued on a mobile device needs to be executed exactly once, in spite of poor network coverage or failures. Finally, mobile applications ought to be flexible in order to accommodate different bearers (transmission technologies: SMS, GSM, GPRS, Bluetooth, Infrared) and interaction styles (synchronous, asynchronous, transactional, one-to-one, or many-to-many).

Mobile application servers go beyond the gateways to provide the infrastructure and the development environment needed to satisfy these requirements. Figure 4-8 shows the conceptual components of a Mobile Application Server (MAS). A MAS is also part of a multi-tier (mostly three-tier) architecture that typically consists of a thin client tier residing on handheld devices, a middle tier consisting of mobile applications and a set of middleware and network services, and a back-end tier consisting of mission-critical databases and applications. Simply sated, MAS = wireless gateway + development and operational facilities. The key components of a MAS are mobile applications, back-end and wireless middleware services, network transport services, and application development environments.

**Mobile Application**. The purpose of a MAS is to support a mobile application. This application contains the business functions specifically developed for the mobile users and typically needs integration with back-end database or business application systems such as mainframe financial accounting systems, manufacturing systems, inventory, ERP (Enterprise Resource Planning) and CRM (Customer Resource Management) systems. This application may be a MEBA or M-P-T-V (Mobile, Positional, Television, Voice) Commerce.

**General Purpose (Back-end) Middleware**. To support the back-end systems, common back-end middleware services such as database and transaction processing are needed. We discussed these and other general purpose middleware services in the “Middleware” Module.

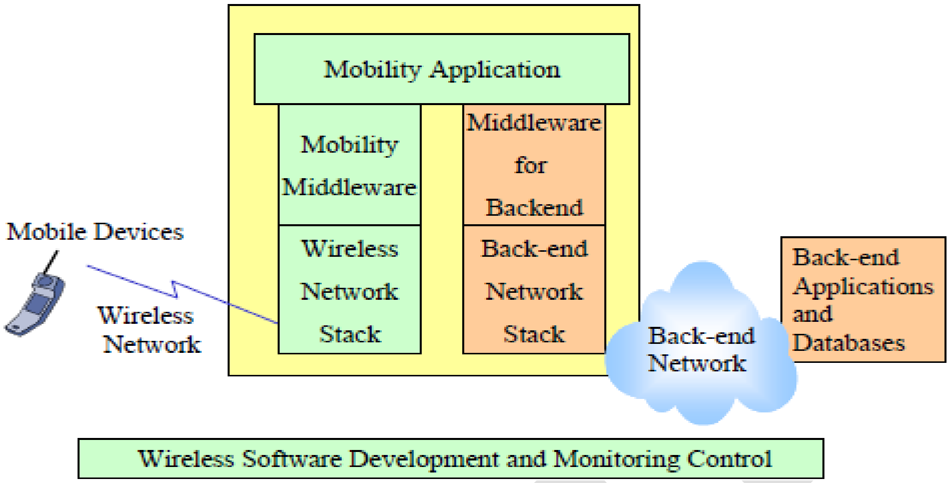
**Mobile Devices**. This may be a cellular phone, notebook, handheld computer, pen computer, PDA, PalmOS compatible PDA, Windows CE/Pocket PC device, or a two-way interactive pager. These devices operate under different mobile operating systems that reside in the mobile device – it may be Windows98/2000/NT, PalmOS, Symbian OS, Win CE (or Pocket PC), EPOC, a specialized OS like Blackberry, or a voice/Web browser.

**Wireless Network.** This may be a wireless LAN, WAN or MAN. These networks are provided by companies such as Cingular (formerly Bell South Wireless Data), Verizon, Sprint, Metricom, Nextel, Bell Mobility (Canada), AT&T (Canada), BT in UK, and NTT

DoCoMo (Japan). To connect computing devices to the wireless network, you need a suitably-configured wireless WAN modem, wireless LAN adapter, or wireless MAN (metro area network) adapter. While wireless network provides true mobility, you may utilize a wireline network for those mobile users who need occasional connection from hotels, motels, or airport lounges. Some of these airports are now offering wireless LAN connectivity to wireline back-end networks.

**Wireless Middleware**. This middleware, also known as mobility middleware, is responsible for handling mobile devices and is the heart of a MAS. This middleware takes raw data from database applications/queries and transforms the data to a specific thin client (or a thick client like a PC) considering its presentation space characteristics and limitations. It breaks the messages into smaller chunks, filters redundant information, and optionally compresses the data, etc. This middleware also provides mobility-specific services such as location, and supports application programming level interfaces (APIs) with specialized communications protocols for wireless. Wireless middleware in most MASs takes the form of a wireless gateway as discussed previously.

**Wireless Software Development and Monitoring/Control Facilities.** Special facilities, such as Software Development Kits (SDKs) are needed to build the mobile applications of the future. These SDKs provide GUI development tools to build mobile application modules that use the wireless middleware APIs. In addition, mobile applications need to be monitored and controlled at run time for errors and load balancing. Wireless software development and monitoring/control facilities are very closely tied to the wireless middleware and are usually packaged with them. For example, the Nokia WAP Server has an SDK and monitoring control commands for WAP.



**Examples of Mobile Application Servers**

Within the conceptual model presented above, a wide range of MASs from different vendors are available commercially. Some mobile application servers are generic web servers with an SDK (Systems Development Kit) or API capability to pull data from back-end systems and send it to a browser-based client software in a handheld device. Other application servers provide a business application with customization capability for wireless access. Still other mobile application servers are extensions of wireless gateways where the vendor decided to add development capabilities to the gateways. Depending on the heritage of the vendor and their core expertise, you can categorize application servers in the following broad classes:

- Generic application servers with a web-based SDK with support for handheld devices and wireless networks. Examples are the Netscape, Microsoft, Sun, and BEA application servers with support for wireless devices.
- Generic database servers with support for mobile devices. Oracle MAS is an example.
- eBusiness/eCommerce Application Servers that have been built specifically to support EC/EB applications. Mobility has been added as a feature to these severs. IBM's WebSphere is an example. We will discuss these servers in the next two chapters.
- Mobility-specific application servers that were built primarily for mobile applications.

**3.7 The Wireless Application Protocol (WAP)**

**Overview**

WAP is a set of protocols to enable the presentation and delivery of wireless information and telephony services on mobile phones and other wireless devices. Two main constraints cause this market to be different from the wireline market. First, the wireless links are typically constrained by low bandwidth, high latency, and high error rates. Second, the wireless devices are constrained by limited CPU power, limited memory and battery life, and the need for a simple user interface WAP specifications address these issues by using the existing standards where possible, with or without modifications, and also by developing new standards that are optimized for the wireless environment where needed. The WAP specification has been designed such that it is independent of the air interface used, as well as independent of any particular device. The key elements of the WAP specification, discussed later in this section, are:

**1. A WAP programming model,** shown in Figure 3.7.1 The model is based heavily on the existing WWW programming model; i.e., a WAP gateway translates between the Web server and the WAP clients.

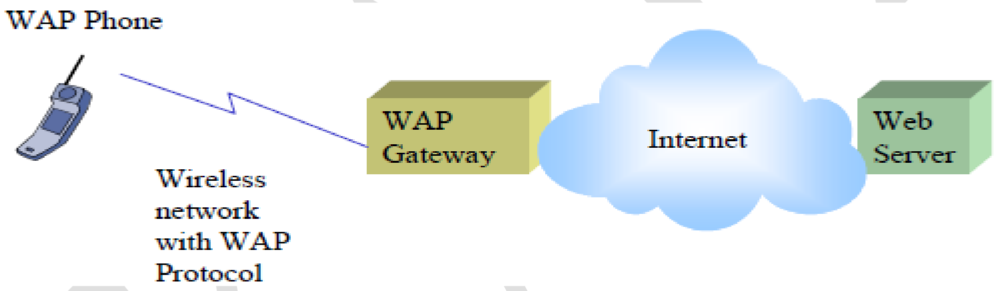


**Figure 3.7.1: WAP Architecture**

**2. A Wireless Application Environment (WAE)** for creating WAP applications and services. The main elements of WAE are:

- A markup language called Wireless Markup Language (WML) that is similar to XML but that has been optimized for wireless links and devices. A scripting language (WMLScript) is also provided.
- Specification of a microbrowser in the wireless terminal. This is analogous to the standard Web browser – it interprets WML and WMLScript in the handset and controls presentation to the user.
- A framework, the Wireless Telephony Applications (WTA) specification, to allow access to telephony services such as call control, messaging, etc. from within the WMLScript applets.

**3. A protocol stack** designed specifically for the wireless environment. WAP supports a lightweight protocol stack to minimize bandwidth requirements, guaranteeing that a variety of wireless networks can run WAP applications. The WAP protocol stack is similar to Internet protocols but is optimized for wireless information pull and push. It supports WAE and consists of (we will discuss these later):

- Wireless Session Protocol (WSP)
- Wireless Transport Layer Security (WTLS)
- Wireless Transaction Protocol (WTP)
- Wireless Datagram Protocol (WDP)
- Wireless network interface definitions

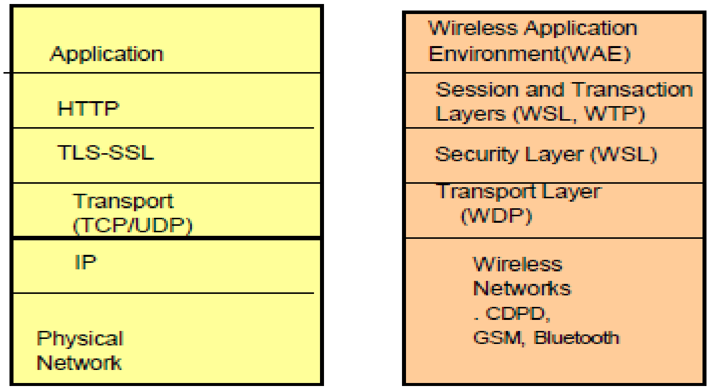

Application
HTTP
TLS-SSL
Transport (TCP/UDP)
IP
Physical Network
Wireless Application Environment(WAE)
Session and Transaction Layers (WSL, WTP)
Security Layer (WSL)
Transport Layer (WDP)
Wireless Networks . CDPD, GSM, Bluetooth

**Figure 3.7.2: WAP Protocol Stack**

Basically, WAP supports development of applications appropriate for handheld devices that are tailored specifically for the wireless Internet. The WAP Forum, now part of the Open Mobility Alliance (OMA), has taken technology elements from TCP/IP, HTTP and XML, optimized them for the wireless environment, and is submitting these optimizations to the W3C standards process as input for the next generations of (XHTML) and HTTP (HTTPNG). Before looking at details, let us briefly review how it works at a high level. Wireless devices communicate through the wireless network to a WAP server. A WAP server converts data or Web pages between WAP and TCP/IP. This conversion lets conventional Web servers send WML pages to wireless devices, which use microbrowsers that let users surf the Web. Tools are emerging that will automate the ability to author content for multiple devices: cell phones, palmtops, and desktops. XML will help this situation by separating information into pure XML content and pure XML style sheet language

(XSL)-based presentation. The point is to design an XML document architecture that separates presentation method, which varies by device, from content. In this way, the XML-based content can be translated to HTML for conventional browsers and to WML for microbrowsers by using different XSL scripts

### 3.8 Overview of IMODE

**What is i-mode?**

While WAP (Wireless Application Protocol) is a standards-based approach for wireless Internet, i-mode, a mobile phone service, also offers continuous Internet access. However, this service is restricted to Japan as of now, with some attempts to make it available to other countries. I-mode (information-mode) was launched in February 1999 by NTT DoCoMo (DoCoMo in Japanese means "anywhere") – a leading cellular phone operator in Japan. Access to websites compatible with i-mode can be achieved at the touch of a button. In addition to phone calls, you can receive email, exchange photographs, receive news and stock quotes, shop online, receive weather forecasts, play online games and access music files online. Every subscriber is given an email ID, which is his or her cellular phone number with the extension "@docomo.ne.jp."

**Key Features of i-mode**

Components required for i-mode services are:

- An i-mode cellular phone, i.e., a phone capable of voice and packet transmission along with a browser installed. I-mode phones are specialized phones with larger windows for multimedia.
- I-mode phones are well-known due to their highly graphic user interfaces.
- Content in cHTML, passed to the browser residing in the i-mode phone.
- An i-mode gateway that translates the cHTML content to the back-end server.
- A packet-switching network that is "always on" – i.e., the end user can turn the phone on and receive the email without having to call a number

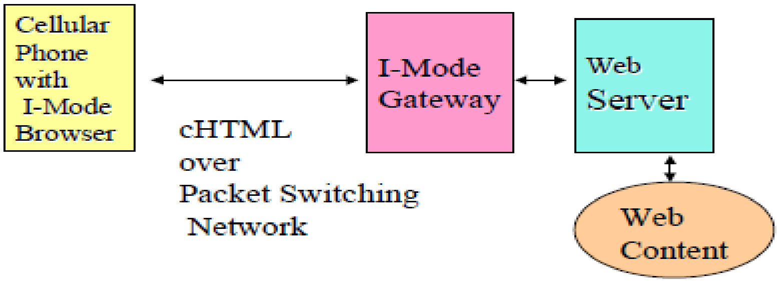

Cellular Phone with I-Mode Browser
I-Mode Gateway
Web Server
cHTML over Packet Switching Network
Web Content

**Figure 3.7.3: i-mode Components**

**cHTML Markup Language**. The markup language that i-mode uses is cHTML (or compact HTML) which is a subset of HTML. It is designed for devices with slower connecting speed.

One main difference between the two languages is that some of the more resource-intensive areas of the code such as tables and frames have been bypassed in cHTML. This reduces the download time to mobile devices. An i-mode-enabled website utilizes pages written in cHTML which are easy to create, for Web designers familiar with HTML.

**i-mode Gateway**: The cHTML content needs to pass through a cHTML gateway before users can access it on their mobile phones using the i-mode browser. When an i-mode- compatible wireless device makes a wireless request, the gateway translates this to the server and back from the server to the wireless device.

**i-mode Browser**. The micro-browser in an i-mode phone is lightweight software designed to run on a handheld device and used to access a cHTML page.

**Packet-Switching Network**. I-mode uses a PDC-P (Personal Digital Cellular-Packet) method of data transmission over the existing PDC network used for ordinary voice traffic. PDC-P is a packet-switched network that is well suited for wireless communication, mainly in Japan. As discussed previously, in a packet-switched network, data is broken into small units called packets and routed over the Net. This mode of transmission, where communication is broken into packets, allows the same data path to be shared among many users in the network. Currently, the rate at which data is being transmitted is 9.6Kbps. But DoCoMo is developing the W-CDMA (Wideband-Code Division Multiple Access technology) a 3G communication system with speeds of 384 Kbps or more. W-CDMA allows high-speed data transmission of video and large-volume data.

**Security**. For security, DoCoMo has formed an alliance with Sun Microsystems to incorporate Sun’s Java, Jini and Java Card technologies into i-mode cellular phones. This provides security for critical applications like online banking and trading, and greater functionality allowing for game downloading and interactivity with other devices.

**i-mode Versus WAP**

The basic difference between WAP and i-mode is that WAP is standards-based while i-mode is not. WAP has strong industry backing from Motorola, Nokia, IBM, Intel, Microsoft, Ericsson, etc. while i-mode is mainly backed by NTT DoCoMo. Other differences are:

- Markup languages are different. I-mode uses cHTML, which is a subset of HTML, while WAP uses WML, which is a subset of XML. Although cHTML is similar to HTML and easier for Web designers to use, XML is the Internet language of the future as HTML has limited capabilities. XML is more tuned to growing standards than cHTML, so growth will be towards XML. WML might incorporate more and more capabilities from XML and will be far stronger than cHTML.
- The level of graphics supported by the two are different. i-mode supports more graphics than WAP. Although WAP supports some amount of graphics, it is not suited for online gaming supported by i-mode phones. The main reason for this is that WAP uses a circuitswitched network at present, while i-mode uses a packet-switched data network, which is more suited to transferring data than circuit-switched networks are.
- Intended audiences may be different. WAP is based on the requirements of people on the move. People on the move would generally not be expected to browse the Net or read large amounts of data or require extensive graphics. I-mode seems to cater to the younger crowd with interest in online games and video. These two audiences could merge as the costs drop and bigger display sizes start appearing on the handsets. Some mobile computing platforms are bridging the gap between WAP and i-mode.

**QualComm's Binary Runtime Environment for Wireless (BREW)**

QualComm created the BREW platform to provide application developers with a platform in which to develop their products, and to allow the same features as J2ME, including crossdevice platform capabilities. The problem is that BREW-enabled applications are mainly dependent on devices with QualComm CDMA chipsets running on a CDMA network.

**So what is so good about BREW?**

BREW addresses a problem that has hampered the wireless industry for a while – nearly every cell phone sold today is expected to be thrown away. Handset manufacturers must load each phone's applications onto the handset at the factory. Further, each application must be custom-built for each individual handset. So how can the applications installed on your current phone be transferred to your new one quickly when you toss the current phone away? Without a way to install new applications on existing phones or to transfer existing applications to new phones, the carriers face a difficult and time-consuming business problem. BREW is intended to simplify application development on CDMA handsets, albeit from QualComm, and to make it possible for end users to download new applications as binary code. In addition, BREW encompasses a distribution method for certifying, downloading, and charging that could speed up the introduction of wireless applications.

The main feature of QualComm's BREW platform is that it is very thin, with a very small footprint. It runs on top of .NET Frameowrk and Visual Studio. BREW code is many times smaller than other platforms due to the sole focus of QualComm on the wireless handsets (rather than a scaled-down version of a product developed for PCs and PDAs). Thus it is more efficient than J2ME code. Due to its focus on binary code, it enables rapid development of a wide variety of downloadable applications. Once developed, these applications can be quickly downlaoded whenever you change your phone or want to get new apps on your existing phone.

### 3.9 Voice Communications

Voice Browsers and Voice XML and other wireless devices. However, it is much more natural in many cases to keep your eyes and hands free by just talking to your telephone. Use of voice communications for conducting business is common for companies. A menu traversed using the phone's keypad is well known to most of us thanks to the IVR (Interactive Voice Response) units that make us all walk through scores of voice menus before we talk to a human being. Development of voice browsers is key to voice communications (see Section 4.7.2 for a discussion of voice browsers). In addition to the voice browser, a collection of markup languages are needed to represent different aspects of voice communications. The World Wide Web Consortium's Voice Browser Working Group is defining several markup languages for applications supporting speech input and output. These markup languages are intended to enable IVR applications across a range of hardware and software platforms. Specifically, the Working Group is designing markup languages for dialog, speech recognition, grammar, speech synthesis, natural language semantics, and a collection of reusable dialog components. These markup languages make up the W3C Speech Interface Framework. Details about this Framework can be found at the W3C website (http://www.w3.org/). Although many markup languages have been introduced for voice communications, the bestknown so far is VoiceXML, created by the VoiceXML Forum (http://www.voicexml.org/). The main goal of VoiceXML is to simplify the task of building IVR applications by automating the menu selection process. Basically the two groups work very closely with each other. The VoiceXML Forum developed the dialog language VoiceXML, which it submitted to the W3C Voice Browser Working Group. The Voice Browser Working Group used those specifications as a model for the Dialog Markup Language.

Voice Browsers According to W3C, "a voice browser is a device (hardware and software) that interprets voice markup languages to generate voice output, interpret voice input, and possibly accept and produce other modalities of input and output." The voice browsers enable users to speak and listen using a telephone or cell phone to access information available on the World Wide Web. These voice browsers accept spoken words as input, and produce speech or replay prerecorded speech as output. In addition to cellular phones and PCs, voice browser hardware processors may be embedded into home appliances practically any electronic or electrical device. Thus voice browsers can be used in an extremely diverse array of mobile as well as non-mobile devices to access Web information through speech. Voice browsers allow people to access the Web using speech synthesis, prerecorded audio, and speech recognition. A voice browser handles scripts written using voice markup languages.

The W3C Voice Browser Working Group (www.w3.org/voice/) was chartered by the World Wide Web Consortium (W3C) in May 1999 to prepare and review markup languages that enable voice browsers. Participants of the Group include the four founding members of the VoiceXML Forum, The Group has developed a Dialog Markup Language (Dialog ML) that is based on the Voice XML language. Attempts to combine the Dialog ML with WML (Wireless Markup Language) are under way. In addition, W3C has developed Synchronized Multimedia Integration Language (SMIL, pronounced "smile") as a presentation language that coordinates the presentation of multiple visual and audio output to the user. Dialog Markup Language coordinates input from the user and output to the user. Eventually the presentation capabilities of SMIL should be integrated with the output capabilities of Dialog Markup Language.

HTML was designed as a visual language with emphasis on visual layout and appearance. Voice interfaces are much more dialog-oriented, with emphasis on verbal presentation and response. Rather than adding HTML with additional features and elements, new markup languages were especially designed for speech dialogs. Thus HTML is not supported by W3C-specified voice browsers. However, some vendors are creating voice-enabled HTML browsers that produce voice instead of displaying text on a screen display. A voice-enabled HTML browser must determine the sequence of text to present to the user as voice, and possibly how to verbally present non-text data such as tables, illustrations, and animations. A voice browser, on the other hand, interprets a script which specifies exactly what to verbally present to the user as well as when to present each piece of information. Voice browsers enable Web-based services from any phone and any device with a voice browser hardware chip. Voice browsers can be a key component of the next generation of call centers and Web portals that combine Internet access with phone access. Users can choose whether to respond by a key-press or a spoken command. Basically, the Web content can be created in XML and can be rendered through XSL for voice browsers, HTML browsers, or WAP browsers (Figure 3.7.2).

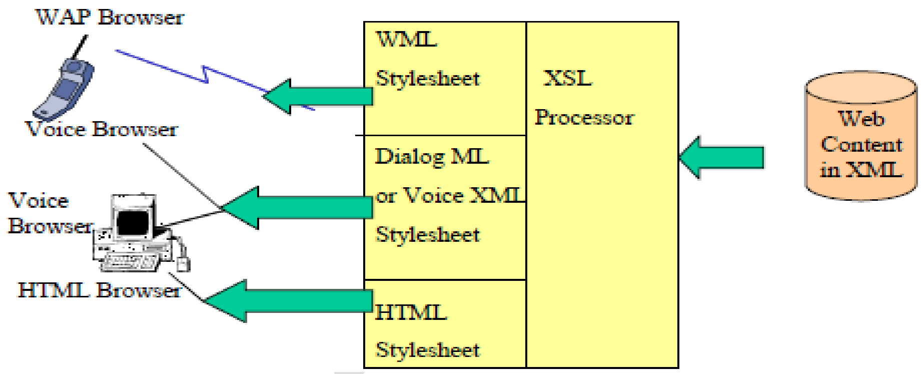


**Figure 3.7.2: Integrating Voice with Other Media**

Finally, a word about multimodal (i.e., voice plus data) interfaces. We are moving towards multimodal interfaces which will need to adjust themselves to the user's current environment and functional abilities. Work on multimodal browsing will address this in the context of user and device profiles

## POSSIBLE QUESTIONS

## UNIT III

### PART-A (Online Examinations)

### PART-B (5 X 6 = 30 Marks)

**(Answer ALL the Questions)**

1. List out the basic features defined in the standard IEEE 802.11 Protocol.
2. Elaborate wireless gateways and voice communication.
3. Explain (i) i-mode (ii) BREW
4. Elaborate the role of XML in wireless web through an example.
5. Explain in detail about wireless application protocol.
6. Enlighten on the 2nd and 3rd generations of cellular networks.
7. What are web services and mobile web services and why are they important to wireless web?
8. Compare and contrast wireless middleware, wireless gateways
9. Compare and contrast WAP with i-mode, wireless Java and BREW.
10. What are web services and mobile web services and why are they important to wireless web?

### PART-C (1 X 10 = 10 Marks)

1. Discuss the architecture of WAP, I-MODE, Wireless JAVA, MMIT, and BREW
2. Compare and contrast wireless middleware, wireless gateways
3. Elaborate the architecture and protocol layers of Bluetooth with a neat diagram.
4. What will be the future of cellular networks beyond 3G?
5. How does a WML application call a Perl script or ASP page? Explain.
6. Give the structure of table in WML and explain with example.

## KARPAGAM ACADEMY OF HIGHER EDUCATION
**Coimbatore - 641021.**
**(For the candidates admitted from 2019 onwards)**

**DEPARTMENT OF COMPUTER SCIENCE,CA & IT**

## WIRELESS AND MOBILE COMPUTING - 19CSP105A

**UNIT III :(Objective Type/Multiple choice Questions each Question carries one Mark )**
**PART-A (Online Examination)**

| S.NO | QUESTIONS | OPTION 1 | OPTION 2 | OPTION 3 | OPTION 4 | KEY |
|---|---|---|---|---|---|---|
| 1 | XSL means | XML Style sheet Language | Extent Style sheet Language | Extensible Style Language | **Extensible Style sheet Language** | **Extensible Style sheet Language** |
| 2 | CDATA means | Copy Data | Cache Data | **Character Data** | None of these | **Character Data** |
| 3 | PCDATA means | Parsed Copy Data | Parsed Cache Data | **Parsed Character Data** | None of these | **Parsed Character Data** |
| 4 | _______ adheres the syntax rules specified by XML | **Well formed Document** | Well formatted Document | Well formed Data | None of these | **Well formed Document** |
| 5 | A________ adheres the rules of DTD and well-formed document | Well formed Document | Well formatted Document | Well formed Data | **Valid Document** | **Valid Document** |
| 6 | EDI means | Electronic Document Interaction | Electronic Data Interface | **Electronic Document Interface** | None of these | **Electronic Document Interface** |
| 7 | XSLTC means | **XSLT Compiler** | XSLT Character | Both a and b | None of these | **XSLT Compiler** |
| 8 | XSLTC converts XSLT style sheet into _______ | Foxpro Code | C Code | Visual Basic Code | **C++ code** | **C++ code** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 9 | MWS means | Mobile Wired Services | **Mobile Web Services** | Mobile Web Search | Mobile Web Security | **Mobile Web Services** |
| 10 | MMIT means | Microsoft Mobile Intranet Tools | Microsoft Mobile Intranet Toolkit | Microsoft Mobile Internet Tools | **Microsoft Mobile Internet Toolkit** | **Microsoft Mobile Internet Toolkit** |
| 11 | UDDI means | Universal Description Discovery and Interface | Universal Description Discovery and Interaction | **Universal Description Discovery and Integration** | Universal Descriptive Discovery and Integration | **Universal Description Discovery and Integration** |
| 12 | SOAP means | Simple Object Access Prototype | **Simple Object Access Protocol** | Simple Object And Protocol | None of these | **Simple Object Access Protocol** |
| 13 | WSDL means | Web Service Distinct Language | Web Secure Description Language | Web Service Description Location | **Web Service Description Language** | **Web Service Description Language** |
| 14 | Example for Mobile OS is | Windows | Linux | Macintosh | **Symbian OS** | **Symbian OS** |
| 15 | CORBA means | Common Resource Break Architecture | Cache Resource Broker Architecture | **Common Resource Broker Architecture** | None of these | **Common Resource Broker Architecture** |
| 16 | MOM means | Mobile Oriented Middleware | Message Oriented Method | Message Outsourcing Middleware | **Message Oriented Middleware** | **Message Oriented Middleware** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 17 | P/S model means | **Publisher/Subscribing Model** | Push/Stop Model | Publisher/Subscriber Model | None of these | **Publisher/Subscribing Model** |
| 18 | JMS means | Java Message Security | Java Mobile Service | **Java Message Service** | None of these | **Java Message Service** |
| 19 | Security Services are | Authenticatio | Identification | **Both a and b** | None of these | **Both a and b** |
| 20 | Performance enhancement of a mobile device based on | Caching | Compression | Security | **Both a and b** | **Both a and b** |
| 21 | MAS means | Middleware Application Survey | Mobile Application Security | **Mobile Application Services** | None of these | **Mobile Application Services** |
| 22 | MAS is part of | **Multi-Tier Architecture** | Two-Tier Architecture | Single-Tier Architecture | Both a and b | **Multi-Tier Architecture** |
| 23 | API means | Application Program Interface | Application Programming Interaction | **Application Programming Interface** | None of these | **Application Programming Interface** |
| 24 | SDK means | Software Development Kits | Software Developer Kit | System Development Kit | **Software Development Kit** | **Software Development Kit** |
| 25 | Traditional MOM models use _________ method. | message passing | **message queuing** | message binding | message alerts | **message queuing** |
| 26 | WTA means | Wired Telephony Applications | **Wireless Telephony Applications** | Wireless Telephony Access | None of these | **Wireless Telephony Applications** |
| 27 | In WAP the _______ model is used to deliver information to the users at certain times | pull | **push** | down | pop | **push** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 28 | WTLS means | **Wireless Transport Layer Security** | Wireless Transport Level Security | Wired Transport Layer Security | None of these | **Wireless Transport Layer Security** |
| 29 | WTP means | Wired Transaction Protocol | **Wireless Transaction Protocol** | Wireless Transmission Protocol | Wireless Transmission Protocol | **Wireless Transaction Protocol** |
| 30 | Wireless middleware is also known as _________ | **mobility middleware** | database middleware | datagram protocol | Wireless Datagram Procedure | **mobility middleware** |
| 31 | OMA means | **Open Mobile Alliance** | Open Mobile Architecture | Open Method Alliance | None of these | **Open Mobile Alliance** |
| 32 | TLS means | Transmission Layer Security | Transport Layer Secrecy | Transport Level Security | **Transport Layer Security** | **Transport Layer Security** |
| 33 | SSL means | Security Socket Layer | Secure Socket Level | **Secure Socket Layer** | Secure Socket Link | **Secure Socket Layer** |
| 34 | The _______ model is used to deliver information to the users at certain times | **Push** | Pull | Both a and b | None of these | **Push** |
| 35 | The _______ model is used to deliver information whenever the users send the query | Push | **Pull** | Both a and b | None of these | **Pull** |
| 36 | The _______ model is used to deliver information whenever the users send the query | Push | **Pull** | Both a and b | None of these | **Pull** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 37 | PAP means | **Push Access Protocol** | Pull Access Protocol | Both a and b | None of these | **Push Access Protocol** |
| 38 | POTA means | Pull Over the Air Protocol | **Push Over the Air Protocol** | Both a and b | None of these | **Push Over the Air Protocol** |
| 39 | ECOM means | **Electronic Commerce** | Electronic Communicatio | Electronic Convergence | Electric Commerce | **Electronic Commerce** |
| 40 | CDPD means | Cellular Digital Packet Device | Cellular Device Packet Data | **Cellular Digital Packet Data** | None of these | **Cellular Digital Packet Data** |
| 41 | ________ converts the WAP protocol stack to the internet stack | **WAP gateway** | Web server | web client | None of these | **WAP gateway** |
| 42 | TDMA means | **Time Division Multiple Access** | Track Division Multiple Access | Time Division Methods of Access | None of these | **Time Division Multiple Access** |
| 43 | To generate the dynamic web page using the following tools ________ | **ColdFusion** | C++ | HTML | None of these | **ColdFusion** |
| 44 | ________ have become commercially available to generate WML codes | XML Editor | C++ Editor | **WML Editor** | None of these | **WML Editor** |
| 45 | J2ME means | Java 2 Micro Environment | Java 2 Mini Edition | Java 2 Mega Edition | **Java 2 Micro Edition** | **Java 2 Micro Edition** |
| 46 | BREW means | **Binary Runtime Environment for Wireless** | Binary Runtime Environment for Wired | Basic Runtime Environment for Wireless | Binary Run level Environment for Wireless | **Binary Runtime Environment for Wireless** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 47 | i-mode means | intellectual-mode | interactive-mode | informational-mode | **information-mode** | **information-mode** |
| 48 | cHTML means | Connectivity HTML | Computer HTML | Conclusive HTML | **Compact HTML** | **Compact HTML** |
| 49 | PDC-P means | Personal Device Cellular-Packet | **Personal Digital Cellular-Packet** | Personnel Digital Cellular-Packet | None of these | **Personal Digital Cellular-Packet** |
| 50 | W-CDMA technology means | **Wideband-Code Division Multiple Access Technology** | Wideband-Code Division Mobile Access Technology | Wideband-Common Division Multiple Access Technology | Wired-Code Division Multiple Access Technology | **Wideband-Code Division Multiple Access Technology** |
| 51 | J2SE means | **Java 2 Standard Edition** | Java 2 Standard Environment | Java 2 Small Edition | Java 2 Selected Edition | **Java 2 Standard Edition** |
| 52 | J2EE means | **Java 2 Enterprise Edition** | Java 2 Environment Edition | Java 2 Employee Edition | None of these | **Java 2 Enterprise Edition** |
| 53 | JVM means | Java Virtual Mobile | Java Virtual Method | Java Virtual Machinery | **Java Virtual Machine** | **Java Virtual Machine** |
| 54 | CVM means | **Compact Virtual Machine** | Compact Virtual Machinery | Connectionless Virtual Machine | None of these | **Compact Virtual Machine** |
| 55 | KVM means | **Kilo Virtual Machine** | Kilo Virtual Machinery | Kilobyte Virtual Machine | None of these | **Kilo Virtual Machine** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 56 | Java uses _________ for security | Black box | **Sandbox** | Security box | White box | **Sandbox** |
| 57 | J2ME applets run in a ________________ | Kilo Virtual Machine | **Compact Virtual Machine** | Both a and b | None of these | **Compact Virtual Machine** |
| 58 | MIDIet means | Mobile Interactive Device-let | Mobile Information Desk-let | **Mobile Information Device-let** | None of these | **Mobile Information Device-let** |
| 59 | A J2ME MIDIet runs in a ________________ | **Kilo Virtual Machine** | Compact Virtual Machine | Both a and b | None of these | **Kilo Virtual Machine** |
| 60 | JCRE means | **Java Card Runtime Environment** | Java Card Run Environment | Java Cache Runtime Environment | None of these | **Java Card Runtime Environment** |

## UNIT-IV

## SYLLABUS

**Wireless LANs** - IEEE 802.11 – MANET – HiperLAN2 - **Wireless Personal Area Networks** - IEEE 802.15 – Home Networks – Blue tooth LANs – Sensor Networks - **Cellular Networks** - Principles – First Generation(1G) Cellular – Paging networks – Second Generation(2G) Cellular – Data over Cellular Networks – Third Generation Cellular (3G) Networks – Beyond 3G

### Wireless LANs – 802.11 and Mobile Ad Hoc Networks

### 4.1 Wireless LAN Overview

### 4.1.1 Principles of Wireless LANs

Figure 4-1 shows a simple wireless LAN configuration. Each mobile device in the wireless LAN has a wireless LAN adapter (in fact a radio transmitter/receiver) that operates in certain frequency ranges. Connectivity to wired networks is provided through an "access point," also known as a local bridge. The access point (AP) can be connected to a wired LAN or to any other type of network for access to corporate databases and/or to the Internet. The mobile devices (e.g., laptops, wireless printers, headsets) connect to the AP when they are in the range of the AP – a cell that may span 10 to 100 meters. Once connected to the AP, the mobile devices can communicate with other devices in the cell or other resources through the AP.

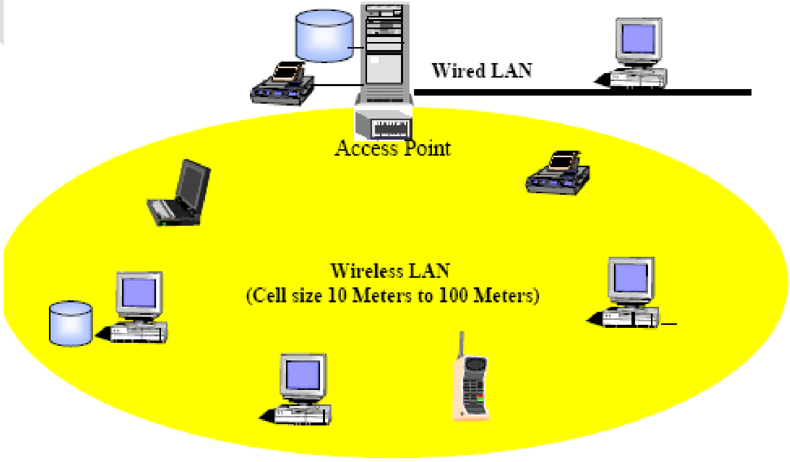


**Figure4-1: A Simple Wireless LAN Configuration**

Wireless LANs augment rather than replace wired LAN networks – they support the final few meters of connectivity between a backbone network and the in-building or on-campus mobile user. The benefits of wireless LANs are:

**Flexibility:** Wireless technology allows the users to roam around a building with their laptops. This is particularly useful for wireless Internet access.

● **Improvements in Productivity**: Wireless LANs can provide LAN users with access to real-time information anywhere in their organization. This improves productivity.

● **Installation Speed and Simplicity**: Wireless LANs can be installed quickly because they eliminate the need to pull cable through walls and ceilings.

● **Reduced Cost:** The initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware. However, the overall installation expenses, especially in dynamic environments, are lower due to savings in cabling costs.

● **Scalability:** Wireless LANs can be configured in a variety of topologies to meet the needs of specific applications and installations. Wireless LANs basically provide all the functionality of wired LANs, but without the physical constraints of the wire itself. Due to these benefits, numerous interesting applications of wireless LANs are possible. Examples of applications can be found in healthcare, manufacturing, car rental, airline, education, defense, restaurants, and many other industries. Sample applications include training sites and universities using wireless LAN connectivity to deliver instruction in any classroom in a building, and doctors and nurses in hospitals using hand-held or notebook computers with wireless LAN capability to deliver patient information instantly. Additional applications include car rental agents greeting the customers in parking lots for convenient car returns, trade show and branch office workers minimizing setup requirements by installing pre-configured wireless LANs, and restaurant waitresses and car rental service representatives providing faster service with real-time customer information input and retrieval.

The wireless LAN industry has grown at a notable rate of between 40 and 60% per year since the mid-1990s and is expected to keep growing at this rate in the future. There are several reasons for this growth. First, a widely accepted wireless LAN standard has been approved by the Institute of Electrical and Electronic Engineers (IEEE). In July 1997, the IEEE 802.11 committee, a subgroup with the IEEE, adopted a worldwide ISO standard for wireless LANs. Second, product prices have decreased dramatically over the past several years. Third, new wireless LAN applications are continually being adopted. Fourth, the mobile computing paradigm is being rapidly adopted by corporate users for office settings. A wide range of WLAN products are now commercially available. A Wireless LAN Alliance (WLANA) has been formed as a consortium of wireless LAN vendors. WLANA provides ongoing education and promotional services about current applications of wireless local area networking and the future of the industry. The Wireless LAN Alliance web site (www.wlana.com) contains a wide range of information.

The main limitation of wireless LANs, as compared to the rival wired LANs, is the security risk of wireless LANs. Horror stories abound, about eavesdropping and connecting to WLANs just by being in their range. We will discuss wireless security in a later chapter. In addition, WLANs are slower. While wireless LANs are achieving 11 to 54 Mbps, the wired LANs such as fast Ethernet have been delivering 100 Mbps for a while. This factor needs to be considered while evaluating the tradeoffs between the two types of LANs. Interoperability, reliability and management is also important in competing with wired LANs. In particular, if a wireless LAN solution is to migrate from the small office home office (SoHo) environment to an enterprise-class organization, it must be robust and secure. 6.2.2 Wireless LAN Technologies at a Glance Table 4-2 displays the highlights of wireless LANs in terms of data rates, distance covered, target applications, frequency allocation, location management, and physical communications. We will use this framework to capture the salient features of all wireless networks as we go along.

**Data Rates and Distance Covered**

WLAN data rates typically range from 11 to 54 Mbps. The data rates could be affected by airwave congestion (number of users), range, and the type of WLAN system used, as well as the latency and bottlenecks on the wired portions of the WLAN.

Most wireless LAN systems use RF because radio waves can penetrate many indoor walls and surfaces. The range (or radius of coverage) for typical WLAN systems is around 100 100 meters. Coverage can be extended and roaming can be supported through microcells and bridges.

**Target Applications**

The applications targeted for WLANs are mostly data applications for offices and home networking situations. Thus WLANs are used commonly for emails, Web browsing, and corporate applications/data access. However, many new voice over 802.11 systems from companies such as Cisco are currently becoming available.

**Frequency Allocations**

WLANs mostly use unregulated bands. For example, 802.11 uses the ISM band. The use of unregulated bands has two major implications: a) the users do not have to pay a usage fee, and b) greater interference from other devices that also use these bands is possible.

**Location Management**

Due to the relatively short communication distances covered by WLANs, the senders and receivers do not travel far from each other. WLAN users typically sit in a spot and walk around in offices or homes. This is quite different from cellular phone users who use the cellular phone while travelling in cars and trains. Thus extensive location management is not needed in WLANs.

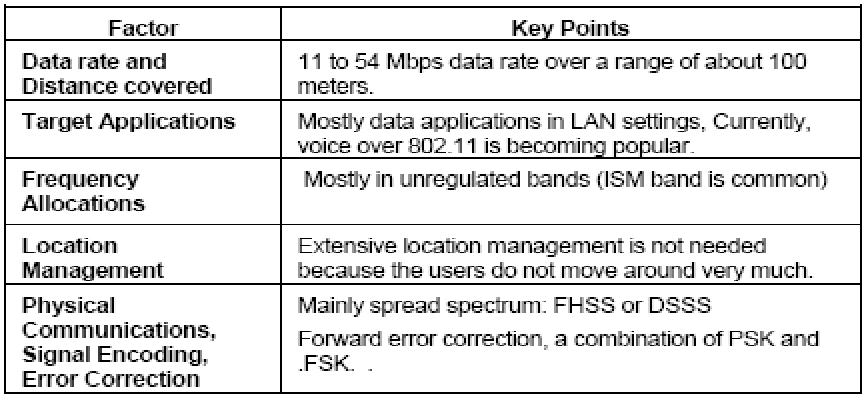
**Physical Communications**

Many serious problems must be faced at the physical communication (layer 1 and 2) by WLANs. First, multiple access mechanisms is important because contention and interference from other devices can be high. One of the main reasons is that WLANs typically operate in unregulated frequency bands which are very crowded. For example, 802.11 LANs (especially the very popular 802.11b and 802.11g) operate in the same band (ISM at 2.4 GHz) as Bluetooth. The techniques used are mainly based on spread spectrum (FHSS or DSSS). Spread spectrum sends signals in such a fashion that only the receiver with the right code can understand it – the others receive a noise. This reduces the interference. In addition, forward error correction (FEC) and ARQ is used for handling errors and a combination of PSK and FSK are used for modulation

### 4.1.2 Wireless LAN Applications and Requirements

Figure 4-2 shows some possible applications of wireless LANs in corporations. This figure shows how wireless LANs can be used to extend wired LANs, provide nomadic access for roaming users, and support ad hoc networking. In building 1, there are two wireless LANs that are linked into a wired LAN through access points. This is an example of ***LAN Extension***. In LAN extensions, the wired LAN is used for backbone that interconnects several wireless LAN stations in large open areas such as a classroom or office. A nomadic station (e.g., a laptop) can connect to wireless LAN1 or wireless LAN2. This, known as ***Nomadic Access,*** provides wireless links between a LAN hub and mobile stations equipped with antennas. One of the wireless LANs (LAN1) uses ***Ad Hoc Networking***, which allows mobile devices to talk to each other without the need for an access point. In this configuration, temporary peerto- peer networks are set up to meet immediate customer needs. For example, an ad hoc network can link computers as a temporary network just for the duration of a meeting. The other wireless LAN (LAN2) uses a ***Master/Slave***, also known as ***Centralized***, LAN configuration. In this case, the devices communicate with each other through a master (an access point in this case). The Wireless LANs can also be used for ***Cross-building Interconnection***: Wireless LANs connect LANs in nearby buildings (in our case between building 1 and 2) by using point-to-point wireless. The devices connected are typically bridges or routers on top of buildings.

**Table 4-2: Basic Information about WLANs**



| Factor | Key Points |
|---|---|
| Data rate and Distance covered | 11 to 54 Mbps data rate over a range of about 100 meters. |
| Target Applications | Mostly data applications in LAN settings, Currently, voice over 802.11 is becoming popular. |
| Frequency Allocations | Mostly in unregulated bands (ISM band is common) |
| Location Management | Extensive location management is not needed because the users do not move around very much. |
| Physical Communications, Signal Encoding, Error Correction | Mainly spread spectrum: FHSS or DSSS<br>Forward error correction, a combination of PSK and .FSK. . |

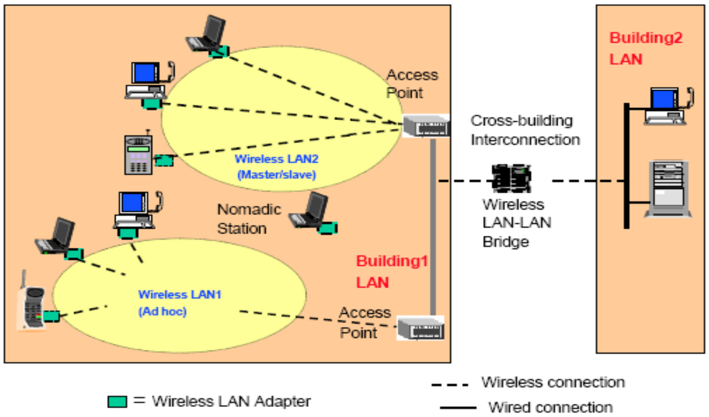


**Figure 4.2 LAN Applications**

To support these and other applications, a wireless network needs to satisfy a wide range of requirements such as the following:

● Connection to backbone LANs must be supported for corporate use. Basically the wireless LAN must be able to connect to a backbone network to provide value.

● Service area for mobile devices should be 100+ meters.

● Battery power consumption should be minimized; i.e., the user devices should go to sleep when not in use.

● Throughput needs to be high; i.e., more work needs to be completed per unit time.

● Transmission robustness and security – i.e., reliable transmission and maintenance of security – are naturally important.

● Collocated network operation must be supported by minimizing interference between neighboring networks. License-free operation should be supported because it is better to operate without licensed frequencies.

● Handoff/roaming and dynamic configurations must be supported. Medium access control (MAC) layer is responsible for these features; i.e., MAC protocol should support smooth handoffs and MAC addressing should support automatic addition and deletion of addresses.

Wireless LAN Technologies

Figure 6-3 shows the key wireless technologies: LAN adapters, access points, and wireless communication technologies.

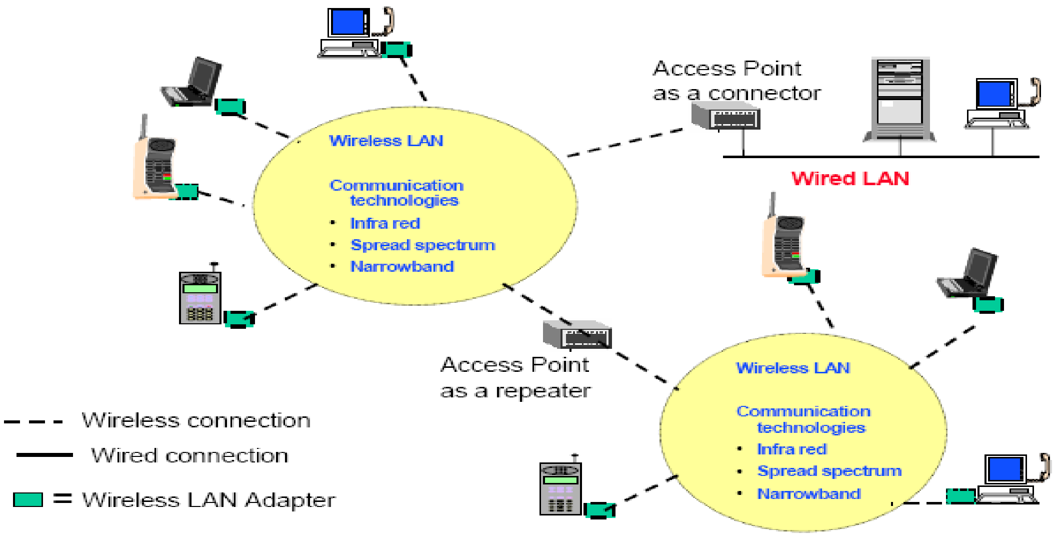


Figure 6-3: Wireless LAN Technologies

### Wireless LAN Adapters

End users access WLANs through wireless LAN adapters, which are implemented as PC cards in laptops, or use appropriate adapters in desktop computers, or fully integrated devices within handheld computers. Wireless LAN adapters are in fact miniature transceivers that provide an interface between the client network operating system (NOS) and the airwaves via an omnidirectional antenna. The nature of the wireless connection is transparent to the NOS.

### Access Points

An access point is a transmitter/receiver (transceiver) device that connects wireless LANs to other wired or wireless networks by using a omnidirectional antenna. It performs two functions: a) it acts as a repeater between two wireless LANs, and b) it acts as a connector (bridge) between wired and wireless networks. For example, an access point can connect your wireless LAN to an Ethernet network from a fixed location using standard Ethernet cable. It can also act as a repeater between two wireless LANs, thus increasing the area covered – it transmits data between the wireless LAN and the wired/wireless networks by using omni directional antennas. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. For wider radio coverage, the access point (or the antenna attached to the access point) is usually mounted high. An example of access points is the Cisco Aironet 340 AP (visit the Cisco site, http://www.cisco.com/ for detailed specification).

### Microcells and Roaming

Wireless communication is limited by how far signals carry for a given power output.

Wireless LANs use cells, called microcells, similar to the cellular telephone system to extend the range of wireless connectivity. At any point in time, a mobile PC equipped with a wireless LAN adapter is associated with a single access point and its microcell, or area of coverage. Individual microcells overlap to allow continuous communication within a wired network. They handle low-power signals and "hand off" users as they roam through a given geographic area. Figure 6-4 illustrates microcells in a wireless LAN environment.

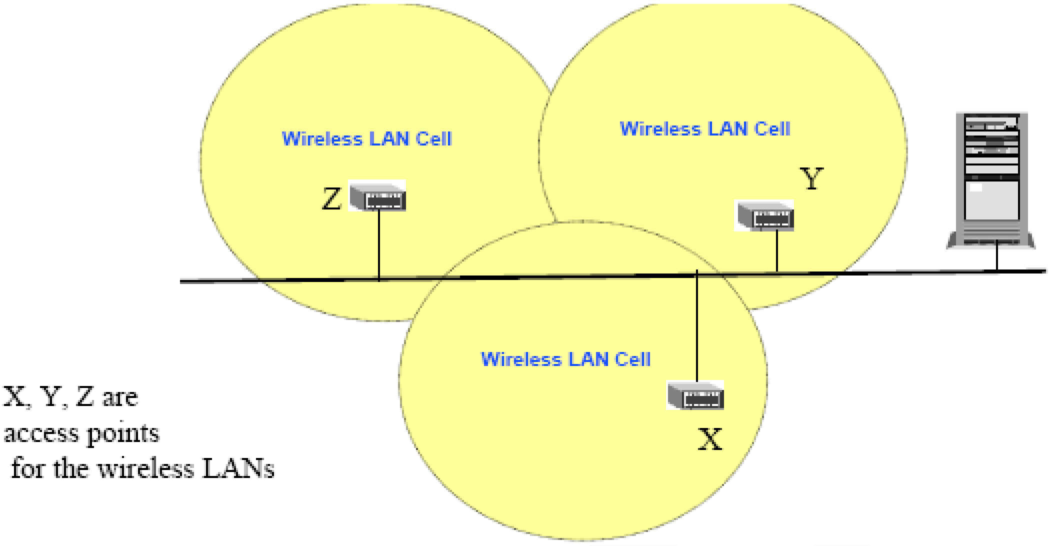


**Figure 6-4: Microcells and Roaming in a Wireless LAN Environment**

### 4.2.2 Wireless Communication Technologies

Wireless LANs use electromagnetic airwaves (typically radio) to communicate between LAN users without relying on any physical connection**.** The data being transmitted is modulated/demodulated on the radio waves (see the sidebar "Modulation/Demodulation for Wireless LANs"). Currently available wireless LANs use one of three signal types to transmit data:

- spread spectrum (most commonly used)
- narrowband microwave
- infrared

In addition, carrier-current LANs, based on existing power lines, are also being used.

**Spread-Spectrum Wireless LANs**

Spread spectrum is most widely used in wireless LANs. These LANs transmit in the ***industrial, scientific, and medical (ISM)*** bands designated by the FCC. These bands, around 2.4 GHz, are not regulated so the LAN suppliers have to worry about preventing interference. This technology was developed for military and intelligence operations (the message is "spread" over a range of frequencies to make it jam-resistant). Spread-spectrum technology, as discussed in a previous chapter, is a wideband radio frequency technique that basically transmits different data bits on different signals, based on a secret scheme, for secure communications. The receiver must know the parameters of the spread-spectrum signal being broadcast to understand the signal. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. In spread-spectrum systems, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is secure and louder. There are two types of spread-spectrum radio: frequency-hopping and direct sequence.

● **Frequency-hopping spread spectrum (FHSS)** uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. For example, the transmitter can transmit 8 bits of data at frequency f1, send the next 12 bits at frequency f2, the next 16 bits at f3, and then back to 8 bits at f1. To an unintended receiver, FHSS appears to be short-duration impulse noise. Wireless LANs such as Bluetooth use FHSS.

● **Direct sequence spread spectrum (DSSS)** generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered (and, of course, the more bandwidth required). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as lowpower wideband noise and is rejected (ignored) by most narrowband receivers. The IEEE 802.11 Wireless Ethernet LAN uses DSSS as well as FHSS. Spread-spectrum LANs are organized around multiple-cell arrangements where within a cell, either peer-to-peer or hub architectures are used. In peer-to-peer topology, no hub is used. Due to this, access is controlled by typical shared access MAC algorithms such as CSMA. These LANs are appropriate for ad hoc LANs. Hub topology, also known as master-slave topology, supports an access point, typically mounted on the ceiling that is connected to the backbone. Hubs may control access and/or serve as multiport repeaters. They can support automatic handoff of mobile stations. Stations in a cell transmit to / receive from hub only, or broadcast using omnidirectional antennas.

**Narrowband Microwave**

Wireless LANs based on **narrowband microwave** technology use the 18.82-to-18.87 GHz and 19.6-to-19.21 GHz frequency ranges. These frequency ranges are licensed by the FCC, which means that a vendor must be approved by the agency to use these frequency ranges. Many wireless LAN vendors consider this to be a restriction. A narrowband radio system transmits and receives user information on a specific radio frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communications channels is avoided by carefully coordinating different users on different channel frequencies. A private telephone line is much like a radio frequency. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. In a radio system, privacy and noninterference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency. Narrowband Microwave LANs use a microwave radio frequency band for signal transmission. These bands have relatively narrow bandwidth and are licensed within specific geographic areas to avoid potential interference. These frequencies are "owned" by various suppliers. For example, Motorola holds 600 licenses in the 18 GHz range. These frequencies cover all metropolitan areas. The main advantage of licensed microwave LANs is that by paying for a license, you are assured that LANs in nearby locations do not interfere with your frequencies. In addition, encrypted transmissions prevent eavesdropping. Unlicensed narrowband microwave LANs use unlicensed ISM spectrum. An early example is the RadioLAN narrowband wireless LAN in 1995 that used low power (0.5 watts or less) within a range of 50 to 100 meters. These LANs operate at 10 Mbps in the 5.8 GHz band.

**Infrared (IR) Wireless LANs**

Infrared signals operate at very high frequencies (300 GHz and above) and behave like ordinary light (they cannot penetrate solid objects). Thus infrared wireless LANs are limited to data transmission along line of sight. Infrared technology is simple and well proven (it is used commonly in remote controls for VCRs and TVs). In addition, infrared signals are not regulated by the Federal Communications Commission (FCC). Technically, infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse (reflective) technology. Inexpensive directed systems provide very limited range (3 to 5 ft.) and typically are used for personal area networks (PANs) such as appliances in the kitchens of the future. High-performance directed IR is impractical for mobile users due to potential obstacles and is therefore used primarily to implement fixed subnetworks. Diffuse (or reflective) IR WLAN systems do not require line-of-sight (you use reflectors such as mirrors). However, you cannot make magic with mirrors too long, thus cells are limited to individual rooms.

In general, the following IR data transmission techniques are used:

● **Directed Beam Infrared** is used to create point-to-point links between wireless nodes. The range depends on emitted power and degree of focusing of the transceiver. A focused IR data link can have a range of kilometers that is not needed for indoor LANs but could be readily used for cross-building interconnection.

● **Ominidirectional Transmission** is used for single base stations in line of sight of all other stations on LAN. The base station transmits in all directions and is typically mounted on a ceiling. The ceiling transmitter broadcasts signals in all directions. This signal is received by IR transceivers and is transmitted back the the IR transceivers. Omnidirectional IR technology is used in the IEEE802.11 LANs.

● **Diffused Infrared**: All IR transmitters are focused and aimed at a point on a diffusely reflecting ceiling. IR radiation strikes the ceiling, is re-radiated omnidirectionally and is picked up by all receivers.

Infrared LANs have several strengths such as the following:

- The spectrum for infrared is virtually unlimited and unused above 300 GHz, thus the possibility of high data rates exists.
- Infrared spectrum is unregulated, thus there is no need to file for licenses.
- Infrared equipment is inexpensive and simple.
- Infrared waves are reflected by light-colored objects, thus ceiling reflection can provide coverage for an entire room.
- Infrared waves do not penetrate walls. Thus infrared LANs are more easily secured against eavesdropping and there is less interference between different rooms.

Drawbacks of infrared LANs are:

- Indoor environments experience infrared background radiation that creates noise.
- Sunlight and indoor lighting also creates background noise.
- Ambient radiation appears as noise.
- Transmitters of higher power are required but are limited by eye safety concerns.

**Carrier-Current LANs – Powerline LANs**

- An interesting development not commonly discussed under wireless LANs is the carrier current LANs (pseudo wireless LANs). These LANs do not require installation of network cables because they use power cables and a powerline modem. These LANs, still under development at the time of this writing, can be used to carry 1 to 2 Mbps of data. An example is the Radioshack Master Console to control coffee machine, lamps, and heating systems.

**Wireless LAN Configurations**

Wireless LANs can be intermixed and configured with disparate networks in different locations of an organization for ease of access. These LANs can be configured as point-to point LANs, peer-to-peer LANs, master-slave LANs, and LANs connected through bridges and access points. Figure 6-5 shows the main configurations

**Point-to-point local area wireless solutions** provide direct wireless links between participating devices. For example, directed beam infrared LANs, discussed previously, create point-to-point links between wireless nodes. Many examples of point-to-point wireless LAN solutions can be found in personal area networks (PANs).

**Wireless PANs (WPANs)** typically cover the few feet surrounding a user's workspace and provide the ability to synchronize computers, transfer files, and gain access to local peripherals. Bluetooth can be thought of as a wireless PAN (not everyone agrees with this view). Figure 6-5 shows a WPAN.

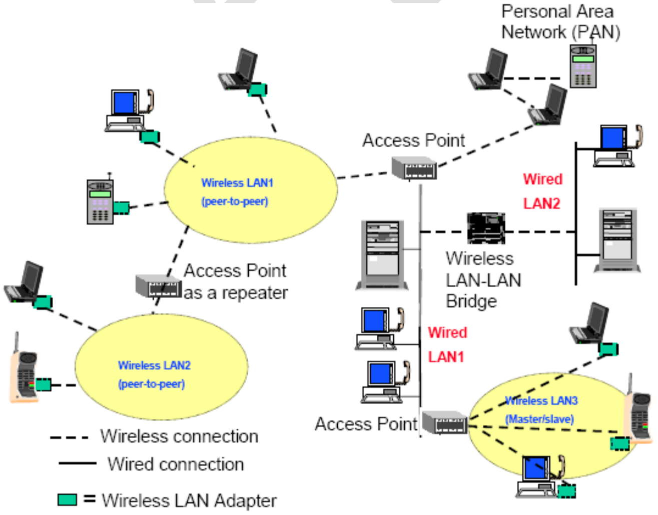

Personal Area Network (PAN)
Access Point
Wired LAN2
Wireless LAN1 (peer-to-peer)
Access Point as a repeater
Wireless LAN-LAN Bridge
Wired LAN1
Wireless LAN2 (peer-to-peer)
Wireless LAN3 (Master/slave)
Access Point
Wireless connection
Wired connection
🟩 = Wireless LAN Adapter

**Figure 6-5: Wireless Configurations in an Enterprise**

**Peer-to-Peer wireless LANs**, also known as ad hoc or independent wireless LANs, are the simplest WLAN configurations. These wireless LANs connect a set of PCs with wireless up a peer-to-peer network. These on-demand networks typically require no administration or pre-configuration. Communications are established between multiple stations in a given coverage area without the use of an access point or server. Standards for peer-to-peer LANs specify the protocols that each station must observe so that they all have fair access to the wireless media. They provide methods for arbitrating requests to use the media to ensure that throughput is maximized for all of the users in the base service set. Wireless LAN1 and LAN2 in Figure 6-5 are examples of peer-to-peer LANs. Section 6.4 gives a closer look at adhoc LANs.

A **Master/slave** (also known as client/server) network uses an access point that controls the allocation of transmission time for all stations and allows mobile stations to roam from cell to cell. The access point is used to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. This arrangement allows for point coordination of all of the stations in the basic service area and ensures proper handling of the data traffic. The access point routes data between the stations and other wireless stations or to and from the network server. Typically WLANs controlled by a central access point will provide better throughput performance. LAN3 in Figure 6-5 is an example of a master/slave wireless LAN. In addition to controlling a wireless LAN, access points can extend the range of independent wireless LANs by acting as repeaters (see Figure 6-5). This effectively doubles the distance between wireless PCs. Multiple access points can link the wireless LANs to the wired network and allow users to efficiently share network resources such as file servers and fast printers. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. Figure 6-5 shows various uses of access points.

A wireless ***LAN-LAN bridge*** is an alternative to cable that connects LANs in two separate buildings. Building-to-Building or LAN-LAN wireless bridges are being used by many industries because you do not have to install and maintain cables between buildings. Wireless LAN-LAN bridging products are available from companies such as Cisco, ELAN, and Wireless Central. The wireless LAN-LAN bridge shown in Figure 6-5 interconnects two LANs in two different buildings.

**The Wireless LAN Stack**

The LAN standards for wired and wireless LANs have been developed by the IEEE 802 Committee. However, some popular LANs such as Bluetooth have been developed by industries. The Committee is organized into the following subcommittees (the number identifies the committee that defines a standard):

- 802.1: High Level Interface
- 802.2: Logical Link Control
- 802.3: CSMA/CD Networks
- 802.4: Token Bus Networks
- 802.5: Token Ring Networks
- 802.6: Metropolitan Area Networks
- 802.7: Broadband Networks
- 802.8: Fiber Optic Networks
- 802.9: Integrated Data and Voice Networks
- 802.10 Virtual LANs
- 802.11 Wireless LANs
- 802.12 Communication media\
- 802.14 Data transport over traditional cable TV network
- 802.15 Personal Area Networks
- 802.16 Wireless Local Loops

Each subcommittee is responsible for developing standards in its designated area, and the published standards are associated with the subcommittee title. For example, the IEEE 802.11 standard for wireless Ethernet was developed by the subcommittee 802.11. Figure 4-6 shows protocol layered views of a WAN and a LAN. For LANs, layer 2 has been divided into two sublayers: Medium Access Control (MAC) and Logical Link Control (LLC).

The **MAC layer** controls the I/O to the physical layer entities. On transmission, this layer assembles the data into a frame with address and error-detection fields. On reception, it disassembles the arriving frame, and performs address recognition and error-detection. This layer also manages the communication over a physical medium such as fiber optics cables.

The **Logical Link Control** layer is responsible for the transfer and formatting of data needed by applications. It basically makes sure that a frame received by the MAC layer is passed to the appropriate application in a station. LLC provides one or more service access points (SAPs) for the applications to interface directly with the LAN.

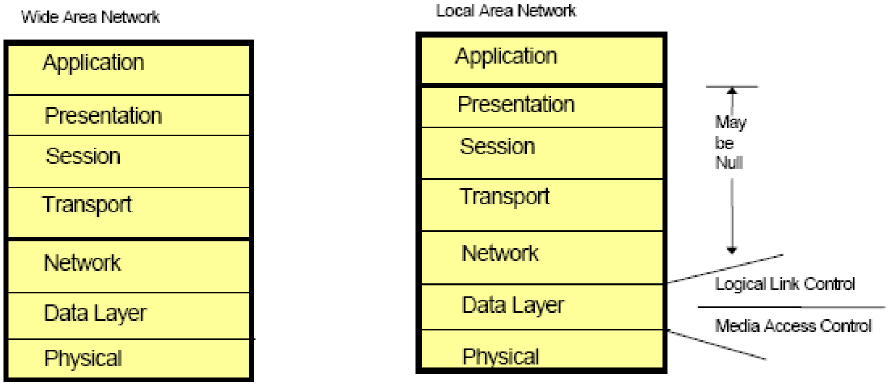
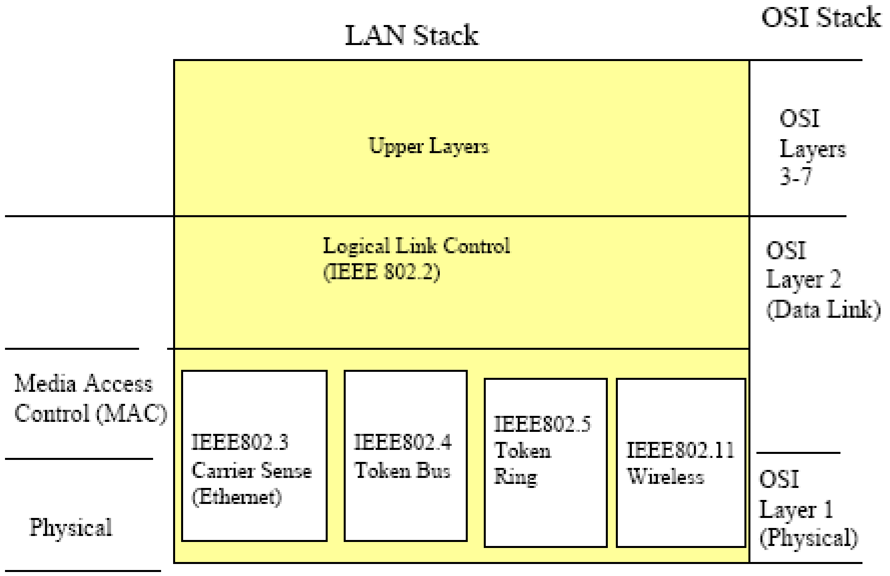


**Figure 4-6: Protocol Stacks for Wide and Local Area Standards**

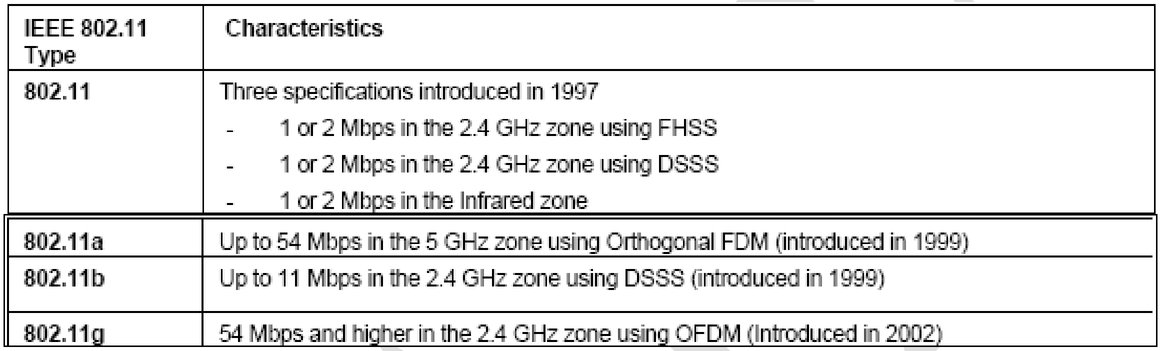
In some cases, it is conceptually easier to think of MAC and LLC layers performing functions that are similar to IP and TCP, respectively. In effect, LLC interfaces with applications in a manner somewhat similar to TCP, while MAC is responsible for delivering messages over the physical LAN media and is similar to IP. The main difference is that LLC-MAC is intended for LANs while TCP-IP is designed for WANs.

Figure 4-7 shows another view of the stack and illustrates how the wireless LAN standard fits with other LAN standards.



### 4.2 IEEE 802.11 Ethernet Standard for Wireless LANs

The IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks Standards Working Group in 1990. The standard has been issued in several stages. The first part, issued in 1997, is simply called 802.11 and operates at 1 and 2 Mbps. The second part, issued in 1999, is called 802.11a and operates at data rates up to 54 Mbps. The third part, also issued in 1999, is known as 802.11b and operates at data rates up to 11 Mbps. The IEEE 802.11g was introduced in 2002 and operates at 54 Mbps. The following table summarizes the main players in the IEEE 802.11 standard family.

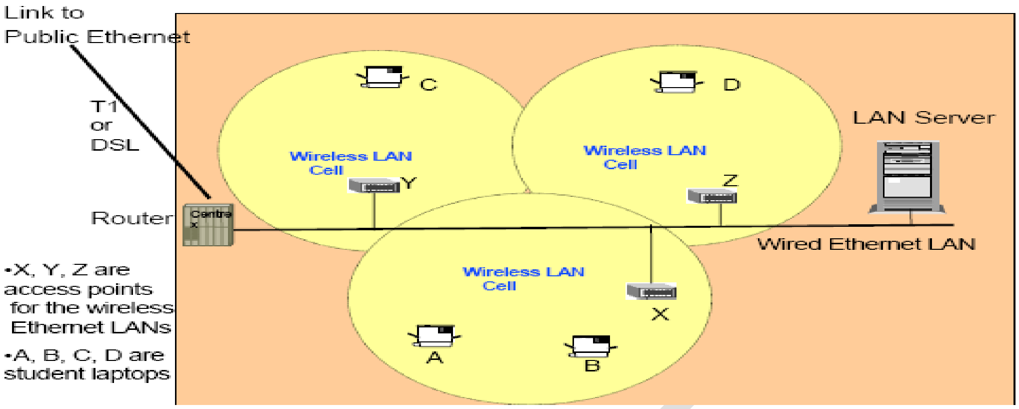


| IEEE 802.11 Type | Characteristics |
|---|---|
| 802.11 | Three specifications introduced in 1997<br>- 1 or 2 Mbps in the 2.4 GHz zone using FHSS<br>- 1 or 2 Mbps in the 2.4 GHz zone using DSSS<br>- 1 or 2 Mbps in the Infrared zone |
| 802.11a | Up to 54 Mbps in the 5 GHz zone using Orthogonal FDM (introduced in 1999) |
| 802.11b | Up to 11 Mbps in the 2.4 GHz zone using DSSS (introduced in 1999) |
| 802.11g | 54 Mbps and higher in the 2.4 GHz zone using OFDM (Introduced in 2002) |

At the time of this writing, 802.11b is very popular although 802.11g is gaining ground steadily. 802.11b, also known as ***Wi-Fi*** (abbreviated from wireless fidelity), supports up to 11 Mbps data rates and provides great vendor interoperability. Thus it competes with the wired Ethernet LANs. You can find Wi-Fi LANs in offices, universities, hotel lobbies, apartment buildings, and “hot spots” at airports and shopping malls. The IEEE802.11b LANs operate in a manner very similar to the wired Ethernet LANs. Of course, there are no cables – the data packets are sent over radio waves. These LANs use the 2.2-to-2.4835 GHz band – the ISM (Industrial, Scientific, and Medical) unlicensed bandwidth reserved for short-range, lowpower devices. As stated previously, a government license is not required to use the devices or the radio transmitter, or to operate other equipment in this frequency range. How do they work? The 802.11b LANs are standardized around the direct-sequence spreadspectrum (DSSS) radio signals. This scheme divides the frequency spectrum into 14 slightly overlapping channels, each 22 MHz wide. So, if each wireless LAN is configured to use one channel, then an office building or a high school can operate 14 wireless LANs in the same physical space. The transmitters in each channel “spread” their signals on the entire 22 MHz bandwidth to improve reception. To discuss how the 802.11b LANs (in fact, all 802.11 LANs) work, let us look at the sample environment shown in Figure 6-8. This environment, commonly found in several small offices, shows several wireless LANs that are connected to a wired LAN to allow the students to access the LAN server as well as the public Internet. The steps in operating this environment are:

- Each access point (AP) is assigned a frequency within the ISM band. The APs X, Y, and Z may be assigned, say, channel 1, 2, and 3 (each 22 MHz). Eleven more APs could be allocated the remaining 11 channels in the same office.
- Each user laptop has an 802.11b card that can send and receive signals in the ISM band. These laptops can thus receive a signal at channel 1 through 14.
- Laptop A and B are in the vicinity of X and thus detect and transmit at signals in channel 1. Similarly, laptop C operates in channel 2 and D in channel 3.
- If laptop A moves from one cell to another (say from X to Y), then its card recognizes a stronger signal in channel 2 and starts listening now to channel 2. This is how the PCs switch from one AP to another.
- Since all 802.11b cards can send and receive information in the ISM band, then theoretically one laptop can establish a connection with any AP by just moving into its range. This presents a serious security problem and requires special approaches such as authentication at AP or encryption

How is interference handled in 802.11b LANs? Wireless Ethernet turns each bit into a pattern of eight radio signals called a “chip.” To achieve high throughput, the transmitters send 64 chips together in one burst. Even if most of the signals are distorted, typically enough will get through to help the receiver assemble an unambiguous result. If there is too much interference, then the receiver asks the transmitter to resend the entire message. If there are too many retries, the receiver may ask the sender to transmit at a lower rate (e.g., 5.5 Mbps or even 1 Mbps). This extra overhead of error checking reduces the effective data rate of wireless Ethernet from 11 Mbps to 10 Mbps (recall that 10 Mbps is the data rate of a wired Ethernet LAN). An attractive feature of 802.11b wireless Ethernet is that about 100 users can be supported on one channel (i.e., each wireless cell can support up to 100 users.



The IEEE 802.11a standard operates in the 5 GHz band and can go up to 54 Mbps. This standard directly competes with the newer 802.11g standard that can also deliver 54 Mbps. Security provisions in 802.11 are addressed in the standard by a complex encryption technique know as the ***Wired Equivalent Privacy Algorithm (WEP).*** WEP protects transmitted data over the RF medium by using a 64-bit seed key and the RC4 encryption algorithm. WEP only protects the data packet information and does not protect the physical layer header. Thus other stations on the network can listen to the control data needed to manage the network but they cannot decrypt the data portions of the packet. Power management is supported at the MAC level for battery operation. Portable stations go to low power "sleep" mode during a time interval defined by the base station.

In many environments, the IEEE802.11b LANs are ideal. But still some problems need to be addressed. Roaming support is a major problem because handoffs from one access point to the next are not clean. While the standards bodies are working on refining the roaming specifications, the wireless LAN users are mostly restricted to desktops and notebooks but not handheld devices. At the time of this writing, Bluetooth and wireless Ethernet LANs (especially 802.11b) are incompatible but share the same 2.4 GHz band.

### 4.3 Mobile Ad-hoc Networks (MANETs)

### 4.3.1 Overview

In Latin, *ad hoc* means "for this purpose only," and is used to imply a temporary setup for a specific purpose. An ad hoc network, also known as ***MANET (Mobile Ad hoc Network***), is a spontaneous, typically wireless local area network in which some of the network devices are part of the network only for the duration of a communications session (e.g., a meeting). The term is used to describe peer-to-peer networks in which new devices can be quickly added or deleted on an as-needed basis. Basically, an ad hoc network is a wireless LAN without an access point (AP). When an AP is present, stations do not communicate on a peer-to-peer basis, thus APs are not part of ad hoc networks (see Figure 4-13).

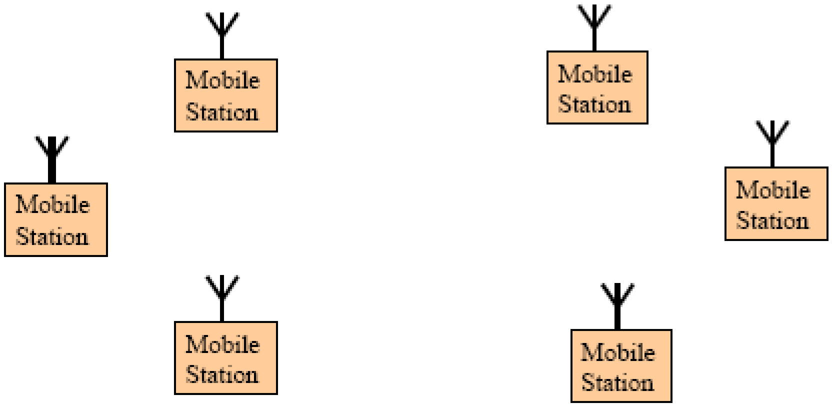


**Figure 4-13: Ad hoc Network**

The main advantage of ad hoc networks is that they are self-organizing wireless networks composed of mobile stations that communicate with each other without a fixed and preplanned infrastructure. Due to this, diverse applications of MANET are possible. MANETs also raise interesting technical problems in routing and media access. Let us review some applications and technical problems.

### 4.3.3 Routing Protocols for Ad Hoc Mobile Wireless Networks

The interconnections between nodes of an ad hoc network are capable of changing on a continual basis. Thus a routing protocol needs to discover routes between nodes on an ongoing basis. This is unlike a wired network where the routes are predetermined. The primary goal of ad hoc network routing protocol is to construct routes with a minimum of overhead and bandwidth consumption. These routing protocols may be categorized as tabledriven or source-initiated on-demand driven.

**The table-driven routing protocols** attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information. The nodes respond to changes in network topology by propagating updates throughout the network to maintain a consistent network view. The areas where they differ are the number of necessary routing related tables and the methods by which changes in network structure are broadcast. A different approach from tabledriven routing is **source-initiated on-demand routing**. This type of routing creates routes only when needed by the sending node. When a sending node requires a route to a destination, it initiates a route-discovery process. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is not changed until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. 6.4.4 Media Access Control Protocols for Mobile Ad Hoc Networks Many applications of ad hoc networks intermix emergency (e.g., medical alert), real-time and non-real-time traffic. This creates different priority classes, each with their own QoS requirements. Access to media to satisfy these sometimes-conflicting QoS requirements is a challenge.

**Carrier-sense multiple access (CSMA)** protocol is a possible candidate for ad hoc wireless networks. CSMA is a simple distributed protocol whereby nodes control their packet transmission attempts based on their perception of the state (busy or idle) of the common radio channel. A station transmits if it finds the channel to be idle (no carrier) and defers transmission if it finds it to be busy (carrier detected). CSMA is very successful in wired LANs (it is the foundation of Ethernet), however it does not provide satisfactory performance in the wireless environment. Furthermore, CSMA cannot provide QoS guarantees to multimedia applications because all traffic sources are treated equally and performance guarantees cannot be provided. In addition, CSMA cannot support different priority classes in ad hoc WLAN or in ad hoc mobile networks.

**Split-channel reservation multiple access (SRMA)** is a protocol specifically designed for wireless networks. SRMA avoids collisions of data packets by introducing a control-signal handshake between the transmitter and the receiver. When node A wishes to send a packet to node B, using Aloha or CSMA, it sends a Request-to-Send (RTS) packet to B. Upon receiving the CTS (Clear-to-Send) packet from B, node A commences transmission of its data packet. SRMA uses separate control channels for RTS and CTS packets and thus can control traffic for QoS.

## 4.4 HiperLAN2

### 4.4.1 Overview

HiperLAN Type 2, or HiperLAN2, is a wireless LAN standard developed by the European Telecommunications Standards Institute (ETSI). The adopters of HiperLAN2 are mainly Europeans who claim that it accommodates current and future evolving wireless network environments, and that it is not merely a wireless LAN solution, but provides superior connectivity technology. A HiperLAN2 Global Forum (http://www.hiperlan2.com/) has been established to promote this standard. Specifically, the following benefits have been highlighted about HiperLAN2:

● Data rate of 54 Mbps

● A high level of security

● QoS capabilities to support virtually any type of service or application

● High and scalable capacity as the number of users increase in the system

● Managed bandwidth with predictable performance for each user and application

● Robust protocols that also optimize the overall throughput of the available radio resource, making it the most spectrum-efficient WLAN technology operating at 5 GHz

● Ease of use through a set of auto-configuration tools

The HiperLAN2 specifications are developed by ETSI BRAN (Broadband Radio Access Network) – a standardization effort within ETSI. HiperLAN2 is a flexible Radio LAN standard designed to provide high speed access (up to 54 Mbps at the physical layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks. It is also intended for private use as a wireless LAN system. It operates in the 5 GHz band – the band that is allocated to wireless LANs worldwide. Thus, it has been claimed that HiperLAN2 has the potential to enable the success of wireless LANs on a global basis.

The HiperLAN2 solution has the following features that proponents claim will be necessary for any long-lasting wireless standard:

● QoS for real-time multimedia communication – at least for operators, it will be vital to find new ways of increasing the revenue streams besides offering plain best-effort Internet services.

● Efficient power-save control for integration into portable devices – if WLAN can’t be integrated into portable devices, the mass consumer market will be left out.

● Medium Access Control (MAC) layer developed and optimized for radio communication on 5 GHz to deliver highest possible throughput over the air interface, and also for when users increase to potentially very high numbers (e.g., a big conference room) within one cell

● Dynamic Frequency Selection (DFS), realizing Automatic Frequency Planning that greatly simplifies the radio network installation and expansion – important to all users, but almost a showstopper if not realized in residential areas

● Plug 'n' play; ideal for multiple access points within an enterprise environment

● Convergence Layer, offering backbone network independence by allowing for interoperability with Ethernet, ATM, IEEE1394 (Firewire) and 3G Mobile systems

● Strong security features with support for individual authentication and per-session encryption keys, including support to use either pre-shared keys or PKI along with DES/3DES

Advanced state of standardization (ahead of 802.11 "g" and "h" extensions) and test specifications HiperLAN2 is extremely well defined to facilitate interoperability and robust protocol operation.

### 4.4.2 HiperLAN2 – Technology Overview

HiperLAN2 is a broadband radio networking technology that allows interconnection into almost any type of fixed network technology. As stated previously, HiperLAN2 supports different levels of Quality of Service (QoS) and security, and is interoperable with existing wired networks such as ATM and TCP/IP.

Figure 4.14 shows a conceptual view of a typical HiperLAN2 radio network. At first glance, HiperLAN2 appears similar to the other WLANs (802.11 and Bluetooth). Mobile Terminals (MT) communicate with Access Points (AP) through wireless technology. The APs are typically connected to a wired LAN for outside access. MTs can also communicate directly with each other to form ad hoc networks and may move around freely within the wireless network. An MT, after login has been performed, can only communicate with one AP at a time, and the AP ensures that the radio network is automatically configured. The terminal requests handover if an AP with a better signal strength is available. Communicating with an AP (master-slave mode) is referred to as Centralized Mode communication in HiperLAN2, and communication between MTs (ad hoc peer-to-peer mode) without passing information via the AP is referred to as Direct Mode.

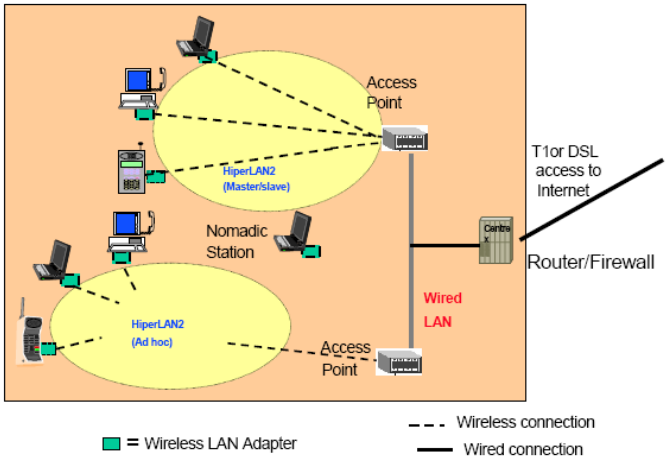


**Figure 4-14: HiperLAN2 Conceptual View**

Figure 4-15 shows the HiperLAN2 protocol stack. The protocol stack is partitioned into two parts: (i) Control Plane and (ii) User Plane. The user plane includes functions for end users while the control plane supervises flow and control of information. The HiperLAN2 protocol consists of three basic layers: (i) Physical Layer, (ii) Data Link Control Layer (DLC), and (iii) Convergence Layer (CL). The Physical Layer (PHY) is virtually the same as for the IEEE 5 GHz standard, 802.11a. The MAC and link sub-layers (part of the DLC layer) provide all the functionality for access control to the medium.

**Layer 1: Physical Layer**

The HIPERLAN type 2 operates in the 5.2 Ghz frequency band with a very high transmission rate of up to 54 Mbps. This is achieved by making use of Orthogonal Frequency Digital Multiplexing (OFDM), which is also used in 802.11a. OFDM transmits high data rate information by dividing the data into several interleaved, parallel bit streams, that are carried by separate sub-carriers. Since the physical layer of HiperLAN2 is very similar to 802.11a, we do not discuss this here.

**Layer 2: Data Link Control Layer**

The Data Link Control Layer supports the logical link between an access point (AP) and the mobile terminals (MTs). The DLC includes functions for medium access and transmission (user plane) as well as terminal/user and connection handling (control plane) and consists of the following sublayers as shown in Figure 4-15:

● **MAC Protocol**. The air interface is based on time-division duplex (TDD) and dynamic time-division multiple access (TDMA). The basic MAC frame structure on the air interface has a fixed duration of 2 ms and comprises transport channels for  broadcast control, frame control, access control, downlink and uplink data transmission and random access. Downlink or uplink traffic consists of PDU trains to and from MTs. A PDU train consists of both user PDUs (long transport channels – LCH) and control PDUs (short transport channel – SCH) to be transmitted and received by one MT. Several other transport channels also exist for broadcast, feedback, etc.

● **Error Control (EC) Protocol.** Selective repeat (SR) ARQ is the Error Control (EC) mechanism that is used to increase the reliability over the radio link. EC refers to detection of bit errors, and the resulting retransmission of U-PDUs if necessary. EC also supports QoS.

● **Radio Link Control Protocol (Signaling and Control).** The RLC protocol gives a transport service for the signaling entities: (i) Association Control Function (ACF) to associate an MT with an AP, (ii) Radio Resource Control function (RRC) to support handoffs and power save functions., and (iii) the DLC User Connection Control function (DCC) for the MT to request user connections. These entities comprise the DLC control plane for the exchange of signaling messages between the AP and the MT.

**Convergence Layer**

The Convergence Layer (CL) adapts to the network environment. Several types of Convergence Layer services have been defined, and new ones can be added if demanded. For example, the Ethernet Convergence Layer makes the HiperLAN2 network operate as a wireless Ethernet extension. This layer has two main functions: (i) adapting service requests from higher layers to the service offered by the DLC and (ii) converting the higher-layer packets with variable or possibly fixed size into a fixed size that is used within the DLC. The generic architecture of the CL makes HiperLAN2 suitable as a radio access network for a diversity of fixed networks, e.g. Ethernet, IP, ATM, UMTS, etc. The structure of the CL includes a common and service-specific part to allow for easy adaptation to different configurations and fixed networks. As a starting point, the HiperLAN2 standard specifies the common part and a service-specific part for interworking with a fixed Ethernet network. The main function of the common part of the convergence layer is to segment packets received from the services.

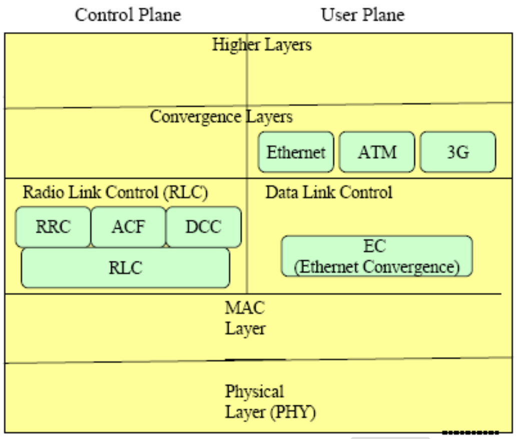


**Figure 4-15: HiperLAN2 Protocol Stack**

### 4.5 Wireless Personal Area Networks

### 4.5.1 Principles and IEEE 802.15 Standards

In principle, a WPAN is a small wireless local area network, thus the basic concepts and technologies discussed in the previous chapter apply. However, as compared to most other wireless networks, WPANs use an ad hoc network model in which there is no need for an access point or a base station for the mobile units to communicate with each other. In a mobile ad hoc network, also known as ***MANET (Mobile Ad hoc Network***), the network devices "discover" each other when they are in each other's company without pre-planning. For example, Bluetooth is based on MANET and supports automatic detection. This is why the Saab's integrated hands-free system, described in the opening case study, is very easy to use – when the driver enters the car with a Bluetooth-enabled mobile phone, the car automatically detects the phone's presence and establishes communication with it. The main advantage of ad hoc networks is that they are self-organizing wireless networks composed of mobile stations that communicate with each other in a peer-to-peer manner without a fixed and pre-planned infrastructure with access points, etc.

Besides the use of MANET, the technical foundations of WPANs are similar to WLANs.

**Data Rates and Distance Covered**

Commonly used WPANs such as Bluetooth deliver 1 Mbps over 10 meter distance. However, there are exceptions. For example, UWB delivers much higher data rates (around 54 Mbps). In addition, sensor networks have much shorter distance -- a few centimeters in case of RFID networks.

**Target Applications**

The applications targeted for WPANs are mostly data applications for short-range radio and home networking situations. These applications are intended for cable replacement and/or communications between appliances, sensors, controllers and other such devices over short ranges. These applications, as stated previously, use the mobile ad hoc network model – there is no need for an access point, although one can be used to connect to the Internet or corporate networks.

**Frequency Allocations**

WPANs mostly use unregulated bands. For example, Bluetooth uses the ISM band. The use of unregulated bands has two major implications: a) the users do not have to pay a usage fee, and b) greater interference from other devices that also use these bands is possible.

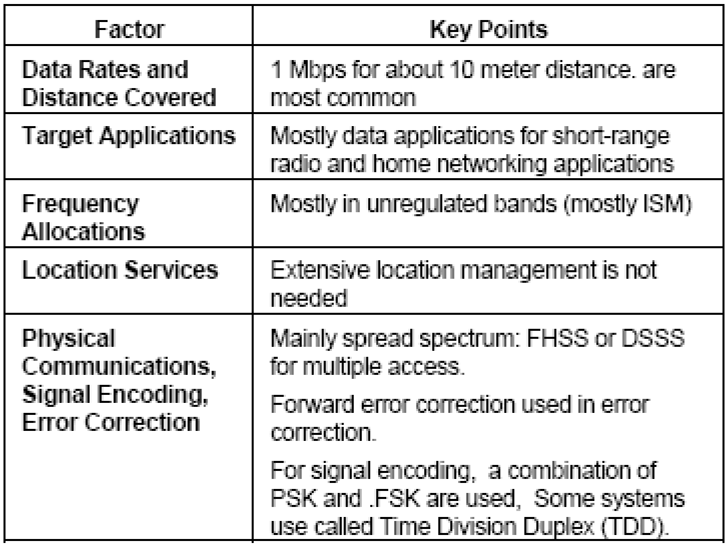
**Location Management**

This is not crucial because in WPANs, mobility of users (senders and receivers) is low. Due to the extremely short communication distances (10 meters) the senders and receivers do not travel far from each other. Thus extensive location management is not needed. In some cases, it is altogether ignored. For example, cordless phones only work in small areas (a home, for example). Once you are outside this range, you have nothing – no roaming support, no handoffs between cells, complete silence.

**Physical Communications**

At the physical communication level, multiple access mechanisms is important because contention and interference from other devices can be high. One of the main reasons is that WPANs typically operate in unregulated frequency bands which are very crowded. For example, Bluetooth operates in the same band (ISM at 2.4 GHz) as the very popular Wi-Fi LANs. The techniques used are mainly based on spread spectrum (FHSS or DSSS). Spread spectrum sends signals in such a fashion that only the receiver with the right code can understand it – the others receive a noise. This reduces the interference. Of course, forward error correction (FEC) and ARQ is used for handling errors. A combination of PSK and FSK is used for modulation. Some short-range systems such as cordless phones use a multiplexing technique called Time Division Duplex (TDD) to support multiple users simultaneously. This scheme is much simpler than the FDMA-TDMA techniques used in cellular and satellite systems. We will discuss TDD later.

**Table4.5-1: Basic Information about WPANs**



| Factor | Key Points |
|---|---|
| Data Rates and Distance Covered | 1 Mbps for about 10 meter distance. are most common |
| Target Applications | Mostly data applications for short-range radio and home networking applications |
| Frequency Allocations | Mostly in unregulated bands (mostly ISM) |
| Location Services | Extensive location management is not needed |
| Physical Communications, Signal Encoding, Error Correction | Mainly spread spectrum: FHSS or DSSS for multiple access.<br>Forward error correction used in error correction.<br>For signal encoding, a combination of PSK and .FSK are used, Some systems use called Time Division Duplex (TDD). |

### 4.6 IEE 802.15 Standards for WPANs – A Quick Overview

Wireless personal area networking is an area of tremendous activity at the time of this writing. The IEEE 802.15 Working Group (WG) has been formed to develop standards for WPANs consisting of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, sensors, control devices, and consumer electronics. As a starting point, the group accepted significant parts of the Bluetooth specification without modification and enriched it with various other features and considerations. The work of 802.15 WG is currently divided into the following task groups:

● **802.15.1 (Bluetooth):** This Task Group has reviewed and provided a standard adaptation of the Bluetooth Specifications.

● **802.15.2 (Coexistence).** This Task Group is developing Recommended Practices to facilitate coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11). Because the WPANs and WLANs have to coexist in many situations, the group is specifying the mutual interferences and the coexistence mechanisms between these two technologies.

● **802.15.3 (WPAN High Rate).** This Task Group is working on a standard for high-rate (20 Mbps or greater) WPANs. This standard is also intended to provide for low-power and low-cost solutions needed in portable consumer digital imaging and multimedia applications.

● **802.15.3a (WPAN Higher Rate).** This Task Group is chartered to develop a new standard for a higher speed (110 Mbps or greater) needed by streaming video and other multimedia applications. A new physical layer (PHY) is being developed by this Task Group for such high data rates.

● **802.15.4 (WPAN Low Rate).** This Task Group is investigating a low data rate solution with multi-month to multi-year battery life and very low complexity. This standard specifies 250 Kbps in the 2.4 GHz band and 20 Kbps-40 Kbps in the 868 MHz bands. The target applications for this standard are sensors, interactive toys, smart badges, remote controls, and home automation. Different Task Groups (TGs) have different levels of activities. For example, the 802.15.1 TG has been in hibernation for a while because the basic work is done. However, the 802.15.3a

### 4.7 Wireless Home Networks:

#### 4.7.1 Overview of Wireless Home Networking

Many people want to wander around their homes while having continual access to a home network. For example, I usually use a laptop sitting in the living room. There is a desktop computer upstairs with cable modem access – a printer is also connected to the desktop. If I want to print a file currently on my PC, then I have to copy the file to a floppy and take it upstairs to print. However, if the file is too large to fit on a floppy, then I have a major problem. I have to disconnect the printer from the desktop, connect it to my laptop and then print. Similarly, if I need Internet access, I have to go upstairs to access the Internet. A wireless home network is an interesting solution for people like me who want to roam around their homes and be connected to a network, a printer, and other such things. The following factors drive the wireless home data networking market:

● The explosive growth and usage of the Internet for delivery of information and entertainment into the home

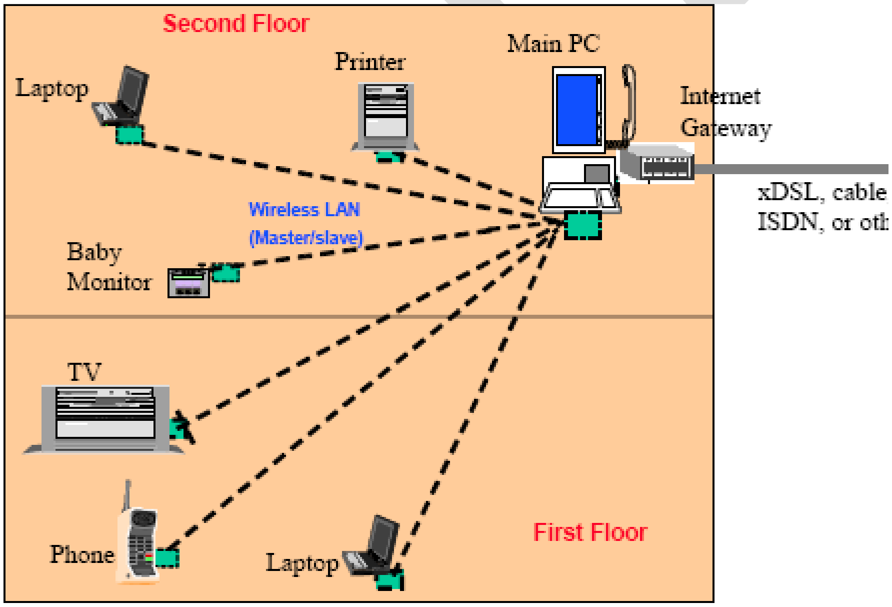
● The widespread emergence of cheaper home PCs (less than $1000) allows middleincome households to obtain a PC if they so wish.

● Home PCs, printers and general computer peripherals can only be reached within a 3-foot diameter. This shortcoming offers a huge opportunity for wireless home networking (who wants 50 feet cables connecting their PCs and computing devices!).

Of course 802.11-based wireless LANs can be used at home, but wireless networks, cheaper and easier to install and maintain, are desirable for home markets. In particular, wireless home networking solutions should satisfy the following requirements [Dhir 2001]:

- No new wiring infrastructures should be needed.
- The solutions must also be simple to install and easy to use.
- Interoperability with other networks such as phone line-based home networks is also essential.
- Solutions need to be economical and home security cannot be compromised.
- Distances should be large enough for consumers who own large households.

Figure 4.6-1 shows a conceptual view of a wireless home network that connects laptops, desktops, printers, phones and other devices though a wireless network. We will revisit this view later. Wireless networks in a household have the obvious advantage of providing access from anywhere at any time. However, security is a big concern because eavesdropping on a wireless network is much easier than on a wired one.



**4.6.1: Conceptual View of a Home Network**

### 4.8 Bluetooth Wireless LANs

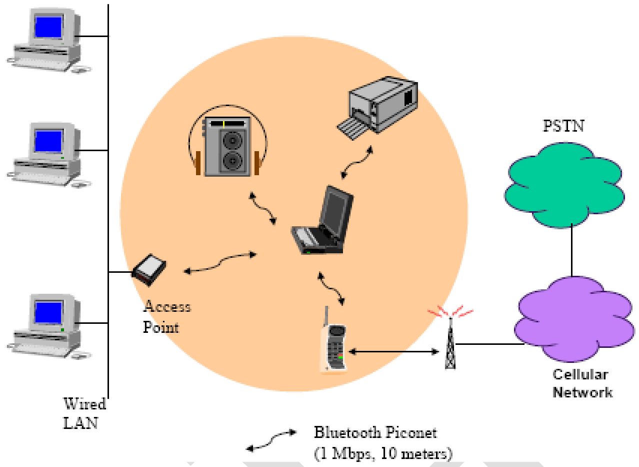
Bluetooth is a medium speed wireless LAN (1 Mbps, 10 meter) specification introduced by Ericsson, IBM, Intel, Nokia, and Toshiba in May 1998. Bluetooth is an always-on, shortrange radio hookup that resides on a microchip and uses the 2.4 GHz ISM band to support devices in small LANs (within 10 meters or less). In reality, Bluetooth can provide up to 720 Kbps of capacity (theoretically up to 1 Mbps). Bluetooth is available globally for unlicensed users and supports an open-ended list of applications that include data, audio, graphics, video, etc.

The main idea of Bluetooth is to develop a way for users to connect a wide range of mobile devices quickly and easily, without cables. For this reason, as we will see, the Bluetooth specification includes numerous “cable replacement” specifications (e.g., the RS232 replacement specification) that allow existing devices to communicate wirelessly without any changes. To ensure that this technology is seamlessly implemented in a diverse range of devices, a special interest group was formed in May 1998 to design a royalty-free, open specification technology, code-named “Bluetooth.” Currently, almost 2000 companies are part of the Bluetooth SIG.

Bluetooth coexists with most wireless LAN solutions. The Bluetooth specification of 1 Mbps is intended as a small form-factor (i.e., few participants), low-cost radio solution that can provide links between highly mobile devices such as mobile phones, mobile computers and other portable handheld devices. This technology, embedded in a wide range of devices to enable simple, *spontaneous* wireless connectivity, is a complement to wireless LANs which are designed to provide *continuous* connectivity via standard wired LAN features and functionality. Bluetooth provides support for the following three broad application areas:

- **Cable replacement** – Bluetooth contains several cable-replacement specifications that eliminate the need for numerous cable attachments. This allows wireless connection to existing devices such as printers and keyboards.
- **Data and voice access points**. Bluetooth supports real-time voice and data transmissions by providing wireless connections to stationary and portable devices.
- **Ad-hoc networking**. A device with Bluetooth radio can automatically establish connection with another Bluetooth-enabled device when in range.

Figure 7-8 shows a simple Bluetooth configuration. Bluetooth was designed to allow lowbandwidth wireless connections to become so simple to use that they seamlessly mesh into your daily life. The idea originated from connecting different devices (e.g., mouse, printer, headset, cellular phone) to a laptop in a small personal area network, called Piconet . The Piconet could, however, be connected to a wired LAN (through an access point), or to a cellular network through a cellular phone.



4.7.1 **A Simple Bluetooth Configuration**

Bluetooth connects and synchronizes automatically with other Bluetooth-enabled devices as they enter the room (or frequency area), including devices that are not in line-of-sight.

Bluetooth technology is comprised of a specially designed microchip with a radio transceiver built into the electronic devices. The range of each radio transceiver is about 10 meters but can be extended through proper amplification and setup to over 100 meters. Bluetooth is able to send both data and voice communications through its transmissions, making voice activated communications more of a reality for mobile users. Due to these attractive features, we may see Bluetooth-enabled thermostats, refrigerators, coffee makers and other devices. Of course, mobile PCs can communicate wirelessly with other mobile PCs, access points, cameras, headsets, and other peripheral devices. Earlier applications of Bluetooth concentrated on cellular phone to PDA or earphone support

## 4.9 Wireless Sensor Networks

Wireless sensor networks (WSNs) typically consist of small, low-powered devices (sensors) that allow the physical environment to be monitored at high resolution. Sensors can be developed to measure temperature, humidity, motion, color changes in a painting, or any other measurable thing. Although most WSNs consist of very small processors communicating over slow wireless networks, WSNs may consist of devices with a wide range of computation, communication, and sensing capabilities. The devices range from relatively powerful systems with PC-class processors to tiny low-power nodes consisting of simple embedded microcontrollers. The WSNs may also use high-bandwidth wireless interfaces (e.g. IEEE 802.11) or, most commonly, low-bandwidth radios operating in the 433 or 916 MHz ISM bands.

What are the best wireless technologies for WSN? The usual suspects are standards like Bluetooth, Wi-Fi, and even cellular. But these provide mid-to-high data rates for voice, PC LANs, and video. Sensors and controls do not need high bandwidth, instead they need low latency and very low energy consumption for long battery lives. The core challenge facing WSNs is managing the tradeoff between local computation and communication. WSNs are typically battery-powered and therefore have a fixed energy budget. In addition, the energy cost to transmit even small amounts of data greatly dominates that of computation. The sensors commonly expend significant CPU cycles to perform local compression, filtering, and aggregation of data in order to save communication overhead.

**Components of a Sensor (Mote)**

As mentioned previously, sensors can be developed to detect almost anything that can be measured. A sensor node *participating* in a sensor network, usually called a ***mote***, typically consists of 3 components; the sensor interface which actually measures the physical attributes such as temperature, the radio interface which communicates with other motes, and the CPU which performs computations and transfers information between the two components (Figure 4-13). Typical commercially available sensor nodes (motes) from companies such as Intel include a 32-bit CPU with a Bluetooth radio interface for network communications. The radio-interface is the most sensitive and power consuming component of a mote because it has to establish communications, detect and correct errors, and send/receive information over the network. The energy consumption of the radio interface influences many WSN design decisions because an attempt is always made to minimize the total energy spent by the network. Thus improvements in wireless network technology and efficient routing protocols greatly impact the sensor nodes.

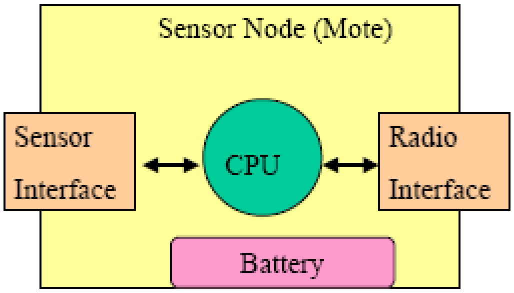


**Figure 4-8: Anatomy of a Sensor Node (Mote)**

### 4.10 Principles of Cellular Networks

Cellular networks are wireless WANs that establish a connection between mobile users. Figure 4.9.1 shows a high level view of a cellular communication network. The cellular network is comprised of many “cells” that typically cover 2 to 20 miles in area. The users communicate within a cell through wireless communications. A Base Transceiver Station (BTS), also known as a Base Station (BS), is accessed by the mobile units in each cell by using wireless communications. One BTS is assigned to each cell. Regular cable communication channels can be used to connect the BTSs to the Mobile Switching Center (MSC), also known as Mobile Telecommunications Service Center (MTSC ). The MSC is the heart of cellular networks – it determines the destination of the call received from a BTS and routes it to a proper site, either by sending it to another BTS or to a regular telephone network. Keep in mind that the communications are wireless within a cell only. The bulk of cell-to-cell communication is carried through regular telephone lines (wireless local loops can be used but are not essential). The MTSC uses two databases called Home Location Register (HLR) and Visitor location Register (VLR) to locate the mobile users.

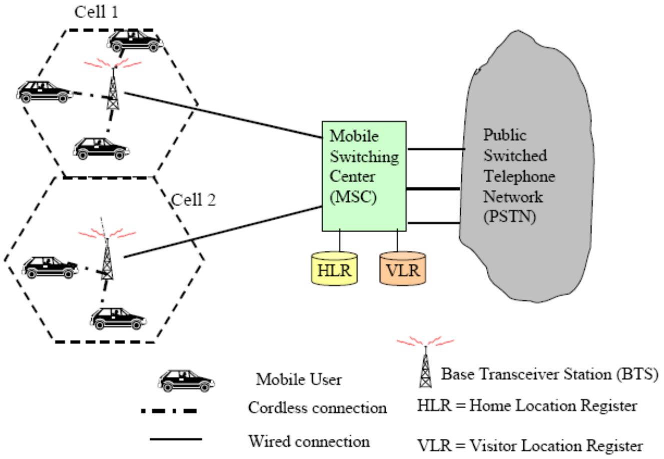

Cell 1
Cell 2
Mobile Switching Center (MSC)
HLR
VLR
Public Switched Telephone Network (PSTN)
Mobile User
Cordless connection
Wired connection
Base Transceiver Station (BTS)
HLR = Home Location Register
VLR = Visitor Location Register

**Fig 4.9.1 A Cellular Communication Network**

The current cellular networks use many different and incompatible standards which rely on different frequency modulation techniques. The focus of the ***third generation wireless systems (3G Networks)*** is on a single network which combines a variety of wireless services. Many initial cellular networks were predominantly analog because mobile communications were primarily targeted for voice users (e.g., cellular phones). However, the use of cellular

## 4.12 Paging Networks

What are Paging Networks?

Paging networks are one of the oldest wireless technologies. They support one-way and two-way alphanumeric messages between callers and pagers (“beepers”). The callers typically call a beeper company and leave a phone number and possibly a short message. Paging networks are being integrated with PDAs (personal digital assistants) like Palm Pilots. An example of paging networks is the BellSouth Clamshell Pager with keyboard.

Paging networks require little bandwidth since each message requires only a single burst of perhaps 30-40 bytes. Thus a satellite with 1 Mbps can handle about 240,000 messages per minute. Older paging protocols operated at 1.2 Kbps (kilobits per second) per channel. Newer protocols such as FLEX (one-way) and ReFLEX (two-way) provide 6.4 Kbps per channel. Paging networks typically operate in the 930-932 MHZ frequency range and are not growing dramatically because paging is now being provided by other devices. Some forecasts at the time of this writing predict that US paging growth will plateau at 20% penetration.

Here are a few characteristics of the paging networks:

- Common applications are personal numeric messaging for call-back, alphanumeric messaging (dispatching and service), and two-way messaging (call dispatching with confirmation).
- Capacity and speed includes 1200 bps for older and 6400 bps for newer systems. The paging networks are slower but have different design criteria for delivering the message within specific time periods.
- Frequency bands used include 800 MHz for older paging networks and 901-941 MHz, with gaps, for newer networks.
- Components of a paging network are a personal paging device, a paging computer/server at the paging operator’s site, and a paging transmitter. These networks may also use satellites for national coverage.
- Coverage is 95% of the US, thanks to many local, regional and national paging network providers.
- Communications protocols supported include FLEX and ReFLEX developed by Motorola for two-way paging.
- Security is low and has not been considered a high priority.

The advantages of paging networks are:

- Very inexpensive
- Easy to operate for sender (from any telephone) and receiver
- Many options for users (numeric, alphanumeric, two-way, message storage)
- Wide coverage at local, regional , national, and international levels
- Good building penetration

The limitations of paging networks are:

- Slow data transfer rate (1200 bps)
- No acknowledgment (two-way paging costs extra)
- Some of the available paging networks are overloaded, causing delays.

### 4.13 Second Generation (2G) Cellular Networks

Second Generation (2G) cellular networks, introduced in the late 1980s, are based on digital transmission. Digital transmissions offer several benefits over analog (see the sidebar "Advantages of Digital Communications for Wireless"). Different approaches to 2G have been developed in the US and Europe. In the US, divergence happened because only one player (AMPS) existed in 1G. Because of this, several players emerged to compete in 2G. Although many players emerged, the following two have survived in the US: ● IS-54 and IS-135: backward-compatible with AMPS frequency allocation (dual mode – analog and digital)

● IS-95: uses spread spectrum

The primary differences between first and second generation cellular networks are: ● Digital traffic channels – first-generation systems are almost purely analog; secondgeneration systems are digital.

● Encryption – all second generation systems provide encryption to prevent eavesdropping.

● Error detection and correction – second-generation digital traffic allows for detection and correction, giving clear voice reception.

● Channel access – second-generation systems allow channels to be dynamically shared by a number of users.

### 4.14 Data Over Cellular Networks

1G cellular system, as indicated previously, is analog because mobile communications were initially developed for voice users (e.g., cellular phones). However, the use of cellular networks to support mobile computing applications is increasing rapidly due to the emphasis on the wireless Web. In particular, as the use of laptop computers, Palm Pilots, PDAs, and sophisticated mobile devices increases, the need to communicate from these mobile computers to access remote databases is also increasing. 2G+ systems use digital communications because digital communications systems can carry voice and data at high quality. If you are a user who wants to send an email over a cellular network, then you have the following choices:

- For an analog network (e.g., 1G), you can use a modem that converts digital data to analog signals.
- For a digital network (e.g., 2G or higher), you can use your digital phone for transmitting data.

- For a packet-switching system, if available, you can use a PAD (packet assembler/disassembler).

An example of a packet-switching system is GPRS, which is built on top of 2G networks.

### 4.15 Third Generation (3G) Cellular Networks

Voice quality comparable to the public switched telephone network. This implies a higher speech quality than the current 2G networks.

- 144 Kbps data rate available to users in high-speed motor vehicles over large areas
- 384 Kbps available to pedestrians standing or moving slowly over small areas
- Support for 2.048 Mbps for office use
- Support for both packet-switched and circuit-switched data services
- Provide a real global system, comprising both terrestrial and satellite components
- More efficient use of the available spectrum in general
- An adaptive interface to the Internet to reflect efficiently the common asymmetry between inbound and outbound traffic
- Support for a wide variety of mobile equipment
- Flexibility to allow the introduction of new services and technologies

### 4.16 Beyond 3G – 4G and 5G Systems

#### 4.16.1 4G Cellular Networks

While 3G wireless networks are still on the design desks, researchers are working on 4G cellular networks with cellular data rates of 20 Mbps and beyond. The high data rate of 4G cellular phones could allow users to watch high-resolution movies and television programs on their cellular phones. A Fourth-Generation Mobile Forum (www.4gmobile.com) has been formed to foster developments in this area. The 4G networks are targeted for 2010 and beyond, although several technical and business questions, including frequency allocations, need to be addressed sooner.

The research towards very high (50 Mbps and above) cellular networks, now known as 4G, started in the 1990s.

Many new technologies and techniques (multiplexing, smart antennas, digital signal processing) are at the core of 4G networks. The physical layer of 4G will be based on Orthogonal Frequency Division Multiplexing (OFDM), and IPv6 will be used at the network layer level. Smart antennas with their ability to adjust based on object movements are an important part of 4G cellular. One of the most difficult questions is determining the frequency spectrum for 4G. The MBS prototype used the 60 GHz band, where there is a large amount of unused bandwidth, but the range is only 100 meters. With such a small range, a nationwide network would require millions of base stations, each one at the center of tiny "picocells". Other experiments include 40 GHz, which would allow larger cells and reduce the cost of building networks. Many companies are involved in this effort. AT&T has initiated a two-phase upgrade of its wireless network on the way to 4G networks, and Nortel is developing features for Internet protocol-based 4G networks. In addition, Alcatel, Ericsson, Nokia and Siemens have found a new Wireless World Research Forum (WWRF) for research on wireless communications beyond 3G. Encouraged by its success with i-mode, DoCoMo expects 4G systems to support the future mobile applications. The enthusiasm for 4G is occurring because the 3G services have proven so disappointing with multitudes of standards and specifications. It is not clear if 4G will be all that different. For example, the crucial issue of frequency bands for 4G needs to be resolved. In addition, many technological, systems engineering, and economic factors need to be hashed to make 4G a business reality. It is nontrivial to develop a 4G architecture that utilizes the best features of W-CDMA, OFDM, smart antennas, and multi-band software-controlled radios.

### 4.16.2 5G Cellular Networks

Some futuristic work on 5G cellular should be mentioned here briefly. The idea is to investigate cellular networks that could deliver data rates above 50 Mbps. At the time of this writing, almost all futuristic work for the next 10 to 20 years is under the umbrella of 5G. The work is proceeding in different directions. Here is a quick recap of the main ideas. Although data rates are the main appeal, the focus is shifting more towards intelligence and learning. A CR is a smart phone that detects the type of conversation and adjusts accordingly. For example, if a CR detects an interview, it could pop up a display suggesting cheaper and better ways of conducting an interview. The phone could learn over time and store the information that the user likes highquality speech when doing interviews. In addition to learning about the user behavior, the software residing on the handset would determine the most appropriate frequency to be used. Thus the handset could choose, instead of the common cellular frequency of 800 to 900MHz band, automatically an ISM band. The handset could also automatically switch between the type of network (cellular, 802.11, or Bluetooth) based on the type of applications. The general vision of 5G is that a PDA, laptop, and automobile would employ the mix of Bluetooth, IEEE 802.11, and cellular standards from 1G to 3G as needed by the user.Another aspect of 5G networks is that special value added services such as location-based services are automatically activated when needed. Of course, there is more emphasis on smart antennas, error correction through turbo codes, and improved signal encoding techniques. One of the main emphasis of 5G cellular is collection of information that can be used to make decisions. For example, it could record the path from your home to work. It could also be measuring the radio propagation, signal strength, and the quality of the different bands as you use your cellular device during the day. It builds an internal database of what it can do when and where.

**POSSIBLE QUESTIONS**

**UNIT IV**

**PART-A(Online Examinations)**

**PART-B (5 X 6 = 30 Marks)**

**(Answer ALL the Questions)**

1. Elucidate the need for sensor networks with examples.
2. Elucidate in detail about generation of cellular networks.
3. Discuss MANET with examples.
4. Elaborate about wireless sensor networks with neat sketch.
5. Elucidate the need for Mobile IP and WWW for wireless.
6. Discuss in detail about wireless sensor networks with neat sketch..
7. Elaborate the architecture and protocol layers of Bluetooth with a neat diagram.
8. What will be the future of cellular networks beyond 3G?
9. Discuss the role of HiperLAN2.
10. Discuss in detail about 3G cellular systems.

**PART-C (1 X 10 = 10 Marks)**

1. Illustrate the architecture of Wireless LANs with neat diagrams
2. Enlighten on the 2nd and 3rd generations of cellular networks.
3. Elucidate the need for Mobile IP and WWW for wireless.
4. Discuss in detail about wireless sensor networks with neat sketch..
5. Discuss in detail about user input operations in WML.
6. Elaborate about functions in WML Libraries with example.

Enable | Enlighten | Enrich
KARPAGAM
ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act, 1956)

# KARPAGAM ACADEMY OF HIGHER EDUCATION
**Coimbatore - 641021.**
**(For the candidates admitted from 2019 onwards)**

**DEPARTMENT OF COMPUTER SCIENCE,CA & IT**

## WIRELESS AND MOBILE COMPUTING - 19CSP105A

**UNIT IV :(Objective Type/Multiple choice Questions each Question carries one Mark )**

**PART-A (Online Examination)**

| S.NO | QUESTIONS | OPTION 1 | OPTION 2 | OPTION 3 | OPTION 4 | KEY |
|---|---|---|---|---|---|---|
| 1 | JCRE runs in a ________ | Kilo Virtual Machine | Compact Virtual Machine | **Java Card VM** | None of these | **Java Card VM** |
| 2 | MIDP means | Mobile Interactive Device Profile | **Mobile Information Device Profile** | Mobile Information Device Program | None of these | **Mobile Information Device Profile** |
| 3 | CDC means | Connectionless Device Configuration | Connect Data Configuration | **Connected Device Configuration** | None of these | **Connected Device Configuration** |
| 4 | CLDC means | Connection-Less Device Configuration | Connect Data Configuration | **Connected Limited Device Configuration** | None of these | **Connected Limited Device Configuration** |
| 5 | Voice Browser is a _________ | **Device** | Data | Both a and b | None of these | **Device** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | Dialing ML means | Dialing Model Language | Dialing Mark Language | **Dialing Markup Language** | None of these | **Dialing Markup Language** |
| 7 | ______________ is based on the Voice XML language | XML | HTML | cHTML | **Dialing ML** | **Dialing ML** |
| 8 | SMIL means | Synchronous Multimedia Interactive Language | **Synchronous Multimedia Integration Language** | Synchronous Mobile Integration Language | Selective Multimedia Integration Language | **Synchronous Multimedia Integration Language** |
| 9 | VoiceXML means | Voice Extensible Mark Language | **Voice Extensible Markup Language** | Voice Extra Markup Language | None of these | **Voice Extensible Markup Language** |
| 10 | VoiceXML supports __________ types of dialogs | **Two** | Three | One | Five | **Two** |
| 11 | Wireless LAN’s data rates typically range between | 7 to 10 Mbps | 62 to 74 Mbps | 55 to 60 Mbps | **11 to 54 Mbps** | **11 to 54 Mbps** |
| 12 | FEC means | Forward Error Compaction | Forward Error Connection | **Forward Error Correction** | Fixed Error Correction | **Forward Error Correction** |
| 13 | FEC means | Forward Error Compaction | Forward Error Connection | **Forward Error Correction** | Fixed Error Correction | **Forward Error Correction** |
| 14 | ISM bands means | Industrial, Security and Medical bands | Industrial, Scientific and Mobile bands | Industry, Scientific and Mobile bands | **Industrial, Scientific and Medical bands** | **Industrial, Scientific and Medical bands** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15 | FHSS means | Frequency-hopping security spectrum | Frequency-hopping speed spectrum | Frequency-hopes spread spectrum | **Frequency-hopping spread spectrum** | **Frequency-hopping spread spectrum** |
| 16 | DHSS means | **Direct sequence spread spectrum** | Direct security spread spectrum | Direct sequence speed spectrum | Dynamic sequence spread spectrum | **Direct sequence spread spectrum** |
| 17 | In WLAN narrow band microwave technology use the following frequency ranges | 18.82-18.87 GHz | 19.6-19.21 GHz | **Both a and b** | None of these | **Both a and b** |
| 18 | Infrared signals operate at WLAN use the following frequency ranges | 18.82-18.87 GHz | **300 GHz and above** | Both a and b | None of these | **300 GHz and above** |
| 19 | FCC means | Federal Communication Cost | Federal Communication Convergence | Federal Co-operative Commission | **Federal Communication Commission** | **Federal Communication Commission** |
| 20 | PAN means | Personal Area Netware ‘ | Personal And Networks | **Personal Area Networks** | Personnel Area Networks | **Personal Area Networks** |
| 21 | Point-to-point links between wireless nodes is used by the following any one of technique | Diffused Infrared | **Direct Beam Infrared** | Ominidirectional Transmission | None of these | **Direct Beam Infrared** |
| 22 | Single base stations between wireless nodes is used by the following any one of technique | Diffused Infrared | Direct Beam Infrared | **Ominidirectional Transmission** | None of these | **Ominidirectional Transmission** |
| 23 | All Infra Red transmitters are focused at a point is used by the following any one of technique | **Diffused Infrared** | Direct Beam Infrared | Ominidirectional Transmission | None of these | **Diffused Infrared** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 24 | Point-to-point local area wireless solutions provide _________ links between participating devices in WLAN | Indirect Wireless | **Direct Wireless** | Both a and b | None of these | **Direct Wireless** |
| 25 | Peer-to-peer Wireless LANs are also called as | Ad hoc Wireless LANs | Independent Wireless LANs | **Both a and b** | None of these | **Both a and b** |
| 26 | A wireless __________ is an alternative to cable that connects LANs in two separate buildings | **LAN-LAN bridge** | LAN-LAN router | LAN-LAN gateway | None of these | **LAN-LAN bridge** |
| 27 | The LAN standards for wired and wireless LANs have been the _______ | IEEE 802.12 | IEEE 802.10 | IEEE 802.15 | **IEEE 802.11** | **IEEE 802.11** |
| 28 | MAC means | Medium Access Communication | Message Authentication Code | Message Access Control | **Medium Access Control** | **Medium Access Control** |
| 29 | LLC means | **Logical Link Control** | Logical Link Communication | Link Level Control | Logical Level Control | **Logical Link Control** |
| 30 | WEP means | Wireless Equivalence Privacy Algorithm | Wired Equivalence Privacy Algorithm | **Wired Equivalent Privacy Algorithm** | Wired Equivalence Protection Algorithm | **Wired Equivalent Privacy Algorithm** |
| 31 | ________ layer deals with the wireless transmission medium | **Physical** | Data Link | Session | Transport | **Physical** |
| 32 | BSS means | Basic Service Security | Basic Secure Set | **Basic Service Set** | None of these | **Basic Service Set** |
| 33 | DS means | Door System | **Distribution System** | Delivery System | None of these | **Distribution System** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 34 | ESS means | Extension Service Security | Extension Secure Set | **Extended Service Set** | None of these | **Extended Service Set** |
| 35 | ________ is used to establish identity of stations to each other | De-authentication | Authorization | Privacy | **Authentication** | **Authentication** |
| 36 | ________ is invoked when existing authentication is terminated | **De-authentication** | Authorization | Privacy | Authentication | **De-authentication** |
| 37 | ________ prevents message contents from being read by an unintended recipient | De-authentication | Authorization | **Privacy** | Authentication | **Privacy** |
| 38 | CSMA/CA protocol means | Carrier-security, multiple access, collision avoidance | Carrier-sense, more access, collision avoidance | **Carrier-sense, multiple access, collision avoidance** | Carrier-sense, multiple access, collision access | **Carrier-sense, multiple access, collision avoidance** |
| 39 | MANETs means | Mobile Ad hoc Netware's | Mobile And Networks | Mobile Ad Networks | **Mobile Ad hoc Networks** | **Mobile Ad hoc Networks** |
| 40 | SRMA protocol means | Split-channel reservation more access | Split-channel reserved multiple access | **Split-channel reservation multiple access** | Simple-channel reservation multiple access | **Split-channel reservation multiple access** |
| 41 | EC protocol means | **Error Control** | Communication | Error Convergence | None of these | **Error Control** |
| 42 | RLC protocol means | **Radio Link Control** | Communication | Radio Level Control | None of these | **Radio Link Control** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 43 | MAP means | Method Access Point | Mobility Access Point | **Mobile Access Point** | Mobile Access Program | **Mobile Access Point** |
| 44 | DSSS means | Direct Sequence Speed Spectrum | **Direct Sequence Spread Spectrum** | Direct Sequence Security Spectrum | Direct Selective Spread Spectrum | **Direct Sequence Spread Spectrum** |
| 45 | FEC means | **Forward Error Correction** | Forward Error Communication | Fixed Error Correction | None of these | **Forward Error Correction** |
| 46 | TDD means | Time Division Dual | **Time Division Duplex** | Time Dual Duplex | None of these | **Time Division Duplex** |
| 47 | ________ task group has reviewed and provided a standard adaptation of the Bluetooth specifications | **802.15.1** | 802.15.2 | 802.15.3 | 802.15.3a | **802.15.1** |
| 48 | ________ task group is developing recommended practices to facilitate coexistence between WLAN and WPAN | 802.15.1 | **802.15.2** | 802.15.3 | 802.15.3a | **802.15.2** |
| 49 | ________ task group is working on a standard for high rate WPANs | 802.15.1 | 802.15.2 | **802.15.3** | 802.15.3a | **802.15.3** |
| 50 | ________ task group is working on a new standard for higher speed WPANs for video and multimedia applications | 802.15.1 | 802.15.2 | 802.15.3 | **802.15.3a** | **802.15.3a** |
| 51 | ________ task group is investigating a low data rate solution with multi-month to multi-year battery life and very low complexity | 802.15.1 | 802.15.2 | 802.15.3 | **802.15.4** | **802.15.4** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 52 | DECT means | **Digital Enhanced Cordless Telecommunications** | Device Enhanced Cordless Telecommunications | Digital Extended Cordless Telecommunications | Digital Enhanced Card less Telecommunications | **Digital Enhanced Cordless Telecommunications** |
| 53 | PWT means | Personnel Wireless Telecom | Personal Wired Telecom | Personal Wireless Telecommunication | **Personal Wireless Telecom** | **Personal Wireless Telecom** |
| 54 | SWAP means | Shared Wired Application Protocol | **Shared Wireless Application Protocol** | Shared Wireless Adaptive Protocol | Shared Wireless Application Program | **Shared Wireless Application Protocol** |
| 55 | ________ layer specifies the requirements for a Bluetooth transceiver operating at 2.4 GHz. | Baseband | **Physical** | Broadband | Session | **Physical** |
| 56 | ________ layer specifies the Bluetooth Link Controller | **Baseband** | Physical | Broadband | Session | **Baseband** |
| 57 | LMP means | **Link Manager Protocol** | Link Message Protocol | Link Manager Program | None of these | **Link Manager Protocol** |
| 58 | HCT means | Host Communication Interface | Host Controller Interaction | **Host Controller Interface** | Home Controller Interface | **Host Controller Interface** |
| 59 | L2CAP means | **Logical Link Control and Adaptation Protocol** | Logical Link Control and Adaptive Protocol | Logical Link Communication and Adaptation Protocol | Logical Level Control and Adaptation Protocol | **Logical Link Control and Adaptation Protocol** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 60 | SDP means | Synchronous Discovery Protocol | Service Discovery Process | Service Distinct Protocol | **Service Discovery Protocol** | **Service Discovery Protocol** |

## UNIT-V

## SYLLABUS

**WML:** Formatting Output – Variables – Input Operations – WML Script – WML Libraries.

### WML

### 5.1 WML - Overview

The topmost layer in the WAP (Wireless Application Protocol) architecture is made up of WAE (Wireless Application Environment), which consists of WML and WML scripting language.

- WML stands for **W**ireless **M**arkup **L**anguage
- WML is an application of XML, which is defined in a document-type definition.
- WML is based on HDML and is modified so that it can be compared with HTML.
- WML takes care of the small screen and the low bandwidth of transmission.
- WML is the markup language defined in the WAP specification.
- WAP sites are written in WML, while web sites are written in HTML.
- WML is very similar to HTML. Both of them use tags and are written in plain text format.
- WML files have the extension ".wml". The MIME type of WML is "text/vnd.wap.wml".
- WML supports client-side scripting. The scripting language supported is called WMLScript.

**WML Versions:**

WAP Forum has released a latest version WAP 2.0. The markup language defined in WAP 2.0 is XHTML Mobile Profile (MP). The WML MP is a subset of the XHTML. A style sheet called WCSS (WAP CSS) has been introduced alongwith XHTML MP. The WCSS is a subset of the CSS2.

Most of the new mobile phone models released are WAP 2.0-enabled. Because WAP 2.0 is backward compatible to WAP 1.x, WAP 2.0-enabled mobile devices can display both XHTML MP and WML documents.

WML 1.x is an earlier technology. However, that does not mean it is of no use, since a lot of wireless devices that only supports WML 1.x are still being used. Latest version of WML is 2.0 and it is created for backward compatibility purposes. So WAP site developers need not to worry about WML 2.0.

**WML Decks and Cards:**

A main difference between HTML and WML is that the basic unit of navigation in HTML is a page, while that in WML is a card. A WML file can contain multiple cards and they form a deck.

When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server. So if the user goes to another card of the same deck, the mobile browser does not have to send any requests to the server since the file that contains the deck is already stored in the wireless device.

You can put links, text, images, input fields, option boxes and many other elements in a card.

**WML Program Structure:**

Following is the basic structure of a WML program:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card id="one" title="First Card">
<p>
This is the first card in the deck
</p>
</card>
<card id="two" title="Second Card">
<p>
Ths is the second card in the deck
</p>
</card>
</wml>
```

The first line of this text says that this is an XML document and the version is 1.0. The second line selects the document type and gives the URL of the document type definition (DTD).

One WML deck (i.e. page ) can have one or more cards as shown above. We will see complete detail on WML document structure in subsequent chapter.

Unlike HTML 4.01 Transitional, text cannot be enclosed directly in the <card>...</card> tag pair. So you need to put a content inside <p>...</p> as shown above.

**WAP Site Design Considerations:**

Wireless devices are limited by the size of their displays and keypads. It's therefore very important to take this into account when designing a WAP Site.

While designing a WAP site you must ensure that you keep things simple and easy to use. You should always keep in mind that there are no standard microbrowser behaviors and that the data link may be relatively slow, at around 10Kbps. However, with GPRS, EDGE, and UMTS, this may not be the case for long, depending on where you are located.

The following are general design tips that you should keep in mind when designing a service:

- Keep the WML decks and images to less than 1.5KB.
- Keep text brief and meaningful, and as far as possible try to precode options to minimize the rather painful experience of user data entry.
- Keep URLs brief and easy to recall.
- Minimize menu levels to prevent users from getting lost and the system from slowing down.
- Use standard layout tags such as <big> and <b>, and logically structure your information.
- Don't go overboard with the use of graphics, as many target devices may not support them.

## 5.2 WML - Formatting

### Line Break:

The <br /> element defines a line break and almost all WAP browsers supports a line break tag.

The <br /> element supports the following attributes:

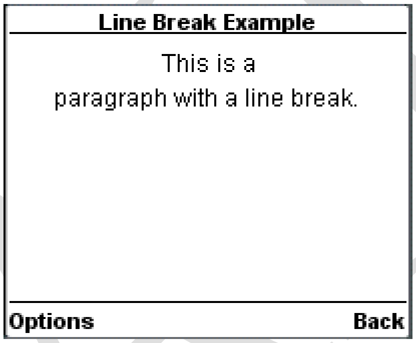
| Attribute | Value | Description |
|---|---|---|
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

Following is the example showing usage of <br /> element.

```
<?xml version="1.0"?>
```

```
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Line Break Example">
<p align="center">
This is a <br /> paragraph with a line break.
</p>
</card>
</wml>
```

This will produce following result:


Line Break Example

This is a
paragraph with a line break.

**Text Paragraphs:**

The <p> element defines a paragraph of text and WAP browsers always render a paragraph in a new line.

A <p> element is required to define any text , image or a table in WML.

The <p> element supports the following attributes:

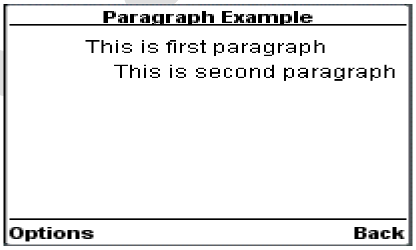
| Attribute | Value | Description |
|---|---|---|
| align | • left<br>• right<br>• center | This is used to change the horizontal alignment of a paragraph. |
| mode | • wrap<br>• nowrap | Sets whether a paragraph should wrap lines or not. |

| | | |
|---|---|---|
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

Following is the example showing usage of <p> element.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Paragraph Example">
<p align="center">
This is first  paragraph
</p>
<p align="right">
This is second  paragraph
</p>
</card>
</wml>
```

This will produce following result:



Paragraph Example

This is first paragraph

This is second paragraph

**WML Tables:**

The <table> element alongwith <tr> and <td> is used to create a table in WML. WML does not allow the nesting of tables

A <table> element should be put with-in <p>...</p> elements.

The <table /> element supports the following attributes:

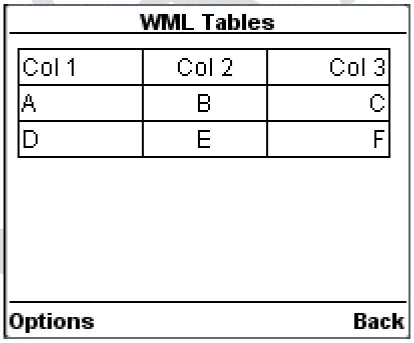
| Attribute | Value | Description |
|---|---|---|
| columns | number | Sets the number of columns in the table |
| align | • L<br>• C<br>• R | To specify the horizontal text alignment of the columns, you need to assign three letters to the align attribute. Each letter represents the horizontal text alignment of a column. The letter can be L, C, or R. For example, if you want the following settings to be applied to your table:<br>• First table column -- Left-aligned<br>• Second table column -- Center-aligned<br>• Third table column -- Right-aligned<br>Then you should set the value of the *align* attribute to LCR. |
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

Following is the example showing usage of <table> element.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="WML Tables">
<p>
<table columns="3" align="LCR">
            <tr>
              <td>Col 1</td>
              <td>Col 2</td>
              <td>Col 3</td>
```

```
        </tr>
        <tr>
          <td>A</td>
          <td>B</td>
          <td>C</td>
        </tr>
        <tr>
          <td>D</td>
          <td>E</td>
          <td>F</td>
        </tr>
</table>
</p>
</card>
</wml>
```

This will produce following result:



WML Tables

| Col 1 | Col 2 | Col 3 |
|---|---|---|
| A | B | C |
| D | E | F |

**Preformatted Text:**

The <pre> element is used to specify preformatted text in WML. Preformatted text is text of which the format follows the way it is typed in the WML document.

This tag preserves all the white spaces enclosed inside this tag. Make sure you are not putting this tag inside <p>...</p>

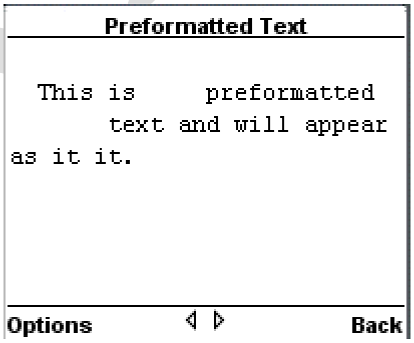
The <pre> element supports following attributes:

| Attribute | Value | Description |
|---|---|---|
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

Following is the example showing usage of <pre> element.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Preformatted Text">
  <pre>
  This is     preformatted
      text and will appear
 as it it.
</pre>
</card>
</wml>
```

This will produce following result:



```
Preformatted Text

  This is     preformatted
       text and will appear
as it it.
```

### 5.3 WML - Variables

Because multiple cards can be contained within one deck, some mechanism needs to be in place to hold data as the user traverses from card to card. This mechanism is provided via WML variables.

WML is case sensitive. No case folding is performed when parsing a WML deck. All enumerated attribute values are case sensitive. For example, the following attribute values are all different: id="Card1", id="card1", and id="CARD1".

Variables can be created and set using several different methods. Following are two examples:

**The <setvar> element:**

The <setvar> element is used as a result of the user executing some task. The >setvar> element can be used to set a variable's state within the following elements: <go>, <prev>, and <refresh>.

This element supports the following attributes:

| Attribute | Value | Description |
|---|---|---|
| name | string | Sets the name of the variable |
| value | string | Sets the value of the variable |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

The following element would create a variable named *a* with a value of 1000:

```
<setvar name="a" value="1000"/>
```

***The input elements:***

Variables are also set through any input element like *input*,*select*, *option* etc. A variable is automatically created that corresponds with the named attribute of an input element.

For example , the following element would create a variable named *b*:

```
<select name="b">
<option value="value1">Option 1</option>
<option value="value2">Option 2</option>
</select>
```

***Using Variables:***

Variable expansion occurs at runtime, in the microbrowser or emulator. This means it can be concatenated with or embedded in other text.

Variables are referenced with a preceding dollar sign, and any single dollar sign in your WML deck is interpreted as a variable reference.

```
<p> Selected option value is $(b) </p>
```

**5.4 WML – Inputs Operations**

WML provides various options to let a user enter information through WAP application.

First of all, we are going to look at the different options for allowing the user to make straight choices between items. These are usually in the form of menus and submenus, allowing users to drill down to the exact data that they want.

**WML <select> Element:**

The <select>...</select> WML elements are used to define a selection list and the <option>...</option> tags are used to define an item in a selection list. Items are presented as radio buttons in some WAP browsers. The <option>...</option> tag pair should be enclosed within the <select>...</select> tags.

This element support the following attributes:

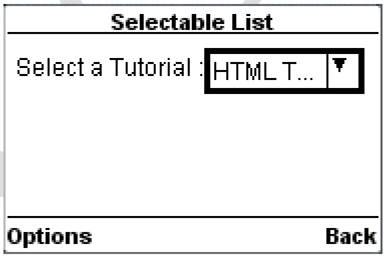
| Attribute | Value | Description |
|---|---|---|
| iname | text | Names the variable that is set with the index result of the selection |
| ivalue | text | Sets the pre-selected option element |
| multiple | • true<br>• false | Sets whether multiple items can be selected. Default is "false" |
| name | text | Names the variable that is set with the result of the selection |
| tabindex | number | Sets the tabbing position for the select element |
| title | text | Sets a title for the list |
| value | text | Sets the default value of the variable in the "name" attribute |
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |

| | | |
|---|---|---|
| id | element ID | A unique ID for the element. |

Following is the example showing usage of these two elements.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Selectable List">
<p> Select a Tutorial :
 <select>
  <option value="htm">HTML Tutorial</option>
  <option value="xml">XML Tutorial</option>
  <option value="wap">WAP Tutorial</option>
 </select>
</p>
</card>
</wml>
```

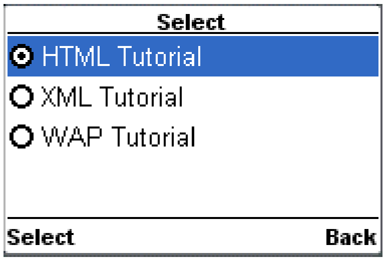
When you will load this program it will show you following screen:



Selectable List

Select a Tutorial : HTML T...

Once you highlight and enter on the options it will display following screen:



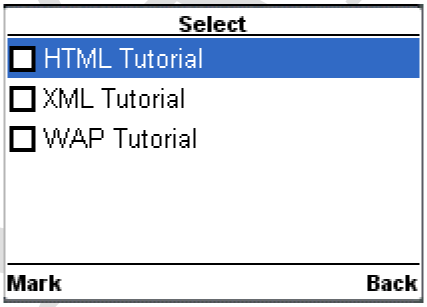
Select

● HTML Tutorial
○ XML Tutorial
○ WAP Tutorial

You wan to privide option to select multiple options then set *multiple* attribute to *true* as follows:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Selectable List">
<p> Select a Tutorial :
 <select multiple="true">
  <option value="htm">HTML Tutorial</option>
  <option value="xml">XML Tutorial</option>
  <option value="wap">WAP Tutorial</option>
 </select>
</p>
</card>
</wml>
```

This will give you a screen to select multiple options as follows:



**WML <input> Element:**

The <input/> element is used to create input fields and input fields are used to obtain alphanumeric data from users.

This element support the following attributes:

| Attribute | Value | Description |
|---|---|---|
| name | text | The name of the variable that is set with the result of the user's input |

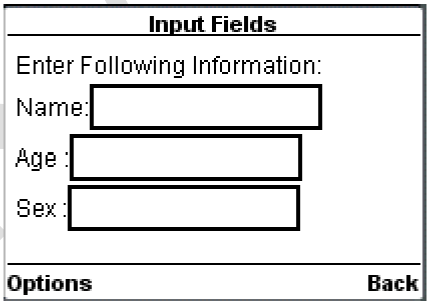
| | | |
|---|---|---|
| maxlength | number | Sets the maximum number of characters the user can enter in the field |
| emptyok | • true<br>• false | Sets whether the user can leave the input field blank or not. Default is "false" |
| format | A<br>a<br>N<br>X<br>x<br>M<br>m<br>*f<br>_nf_ | Sets the data format for the input field. Default is "*M".<br>A = uppercase alphabetic or punctuation characters<br>a = lowercase alphabetic or punctuation characters<br>N = numeric characters<br>X = uppercase characters<br>x = lowercase characters<br>M = all characters<br>m = all characters<br>*_f_ = Any number of characters. Replace the _f_ with one of the letters above to specify what characters the user can enter<br>_nf_ = Replace the _n_ with a number from 1 to 9 to specify the number of characters the user can enter. Replace the _f_ with one of the letters above to specify what characters the user can enter |
| size | number | Sets the width of the input field |
| tabindex | number | Sets the tabbing position for the select element |
| title | text | Sets a title for the list |
| type | • text<br>• password | Indicates the type of the input field. The default value is "text".<br>Password field is used to take password for authentication purpose. |
| value | text | Sets the default value of the variable in the "name" attribute |
| xml:lang | language_c | Sets the language used in the element |

| | | |
|---|---|---|
| | ode | |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

Following is the example showing usage of this element.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Input Fields">
<p> Enter Following Information:<br/>
 Name: <input name="name" size="12"/>
 Age :  <input name="age" size="12" format="*N"/>
 Sex :  <input name="sex" size="12"/>
</p>
</card>
</wml>
```

This will provide you following screen to enter required information:



**WML <fieldset> Element:**

The <fieldset/> element is used to group various input fields or selectable lists.

This element support the following attributes:

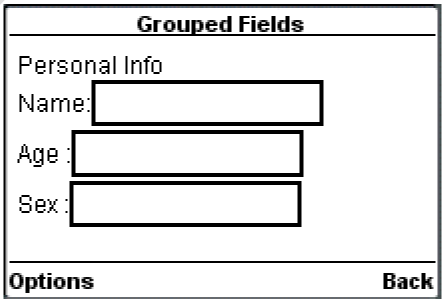
| Attribute | Value | Description |
|---|---|---|

| | | |
|---|---|---|
| title | text | Sets a title for the list |
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

Following is the example showing usage of this element.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Grouped Fields">
<p>
<fieldset title="Personal Info">
 Name: <input name="name" size="12"/>
 Age :  <input name="age" size="12" format="*N"/>
 Sex :  <input name="sex" size="12"/>
</fieldset>
</p>
</card>
</wml>
```

This will provide you following screen to enter required information. This result may differ browser to browser.



Grouped Fields

Personal Info

Name:

Age :

Sex :

**WML <optgroup> Element**

The <optgroup/> element is used to group various options together inside a selectable list.

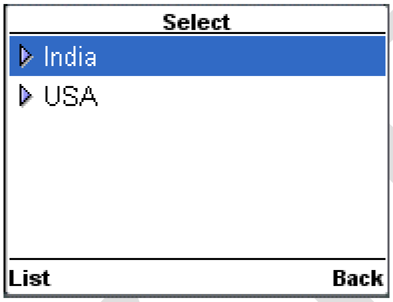
This element support the following attributes:

| Attribute | Value | Description |
|---|---|---|
| title | text | Sets a title for the list |
| xml:lang | language_code | Sets the language used in the element |
| class | class data | Sets a class name for the element. |
| id | element ID | A unique ID for the element. |

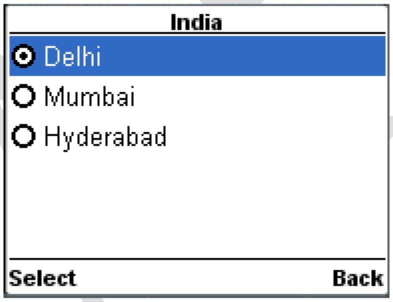
Following is the example showing usage of this element.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card title="Selectable List">
<p>
 <select>
   <optgroup title="India">
    <option value="delhi">Delhi</option>
    <option value="mumbai">Mumbai</option>
    <option value="hyderabad">Hyderabad</option>
   </optgroup>
   <optgroup title="USA">
    <option value="ohio">Ohio</option>
    <option value="maryland">Maryland</option>
    <option value="washington">Washingtone</option>
   </optgroup>
 </select>
</p>
</card>
</wml>
```

When a user loads above code then it will give two options to be selected:



When a user select any of the options then only it will give final options to be selected. So if user selects India then it will show you following options to be selected:



### 5.5 WMLScript Introduction

WMLScript (Wireless Markup Language Script) is the client-side scripting language of WML (Wireless Markup Language). A scripting language is similar to a programming language, but is of lighter weight. With WMLScript, the wireless device can do some of the processing and computation. This reduces the number of requests and responses to/from the server. In the old days, fewer round-trips can improve the performance of your WAP site significantly since data transmission over wireless networks is slow. Today, the performance gained may not be so significant any more as data transmission speed has improved a lot. However, you may still find WMLScript useful since putting some operations at the client-side can reduce the load of your servers. WMLScript is based on

ECMAScript (European Computer Manufacturers Association Script), which is JavaScript's standardized version. So, the syntax of WMLScript is very similar to JavaScript. (In case you do not know, JavaScript is a scripting language commonly used on the web.) If you have some programming experience with JavaScript, you should be able to learn WMLScript quickly. You may glance through or even skip some parts of this WMLScript tutorial.

A major difference between JavaScript and WMLScript is that JavaScript code can be embedded in the HTML markup, whereas WMLScript code is always placed in a file separated from the WML markup. URLs are used to refer to the actual WMLScript code in the WML document. WMLScript has a number of standard libraries. They contain a lot of useful functions that you should get familiar with. We will talk about them in later parts of this WMLScript tutorial. One common use of WMLScript is to validate form data. Another common use is to display message boxes to give alerts and error messages or to ask for confirmation of actions (no round-trip is needed for showing message boxes, which helps save bandwidth and improve the WAP application's response time).

**WMLScript MIME Type and File Extension**

WMLScript files have the extension ".wmls". The MIME type is "text/vnd.wap.wmlscript".

**5.6 WML Script Application**

**Validating Form Data**

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.3//EN"
"http://www.wapforum.org/DTD/wml13.dtd">

<wml>
  <card id="card1" title="Registration Form">
    <p>
      <big>Registration Form</big><br/>
      Notice: Fields with * are required.<br/><br/>
      <b>$(errorMsg)</b><br/>
      * User name:<br/>
      <input name="username"/><br/>
      * Password (min. 8 characters):<br/>
      <input type="password" name="password"/><br/>
      * Email:<br/>
      <input name="email"/><br/>
      Name:<br/>
      <input name="name"/><br/>
      Birthday (MMDDYYYY):<br/>
      <input name="birthday" format="NNNNNNNN" emptyok="true"/><br/><br/>
      <a href="validateFormEg1.wmls#validate()">Submit Form Data</a>
    </p>
  </card>
</wml>
```

The above WML card is used to collect data. If the user clicks the "Submit Form Data" anchor link, the WMLScript function *validate()* will be executed.

The WML variable *errorMsg* is used to store the error message to be shown to the user. If the *validate()* function finds that the form data is not valid, it will assign an error message to the WML variable *errorMsg* and refresh the current WML card so that the user can know what goes wrong and can then make corrections.

We want to impose a number of restrictions on the form data. They are listed below:

1. The username, password and email fields cannot be empty.
2. The password field must contain at least eight characters since a short password is less secure.
3. The email field must contain the @ character that divides the string into two parts.
4. The birthday field must contain 8 numeric characters.
5. The birthday field must contain a valid date in the MMDDYYYY format. For example, 01401990 is not a valid date since a month does not have 40 days.

Here is the WMLScript function *validate()* that is called to check whether the form data follows the above restrictions:

```
extern function validate()
{
  var form_username = String.trim(WMLBrowser.getVar("username"));
  var form_password = String.trim(WMLBrowser.getVar("password"));
  var form_email = String.trim(WMLBrowser.getVar("email"));
  var form_name = String.trim(WMLBrowser.getVar("name"));
  var form_birthday = String.trim(WMLBrowser.getVar("birthday"));
  if (""==form_username){
    WMLBrowser.setVar("errorMsg", "The User Name field must not be empty.");
    WMLBrowser.refresh();
    return;
  }
  if (""==form_password){
    WMLBrowser.setVar("errorMsg", "The Password field must not be empty.");
    WMLBrowser.refresh();
    return;
  }
  if (""==form_email){
    WMLBrowser.setVar("errorMsg", "The Email field must not be empty.");
    WMLBrowser.refresh();
    return;
  }
  if (String.length(form_password) < 8){
    WMLBrowser.setVar("errorMsg", "The password must contain at least 8 characters since a short password is less secure.");
    WMLBrowser.refresh();
    return;
  }
  if (!isEmailValid(form_email)){
    WMLBrowser.setVar("errorMsg", "The email address's format is invalid.");
    WMLBrowser.refresh();
    return;
  }  if (""!=form_birthday && !isDateValid(form_birthday)){
    WMLBrowser.setVar("errorMsg", "The date in the Birthday field is invalid.");
    WMLBrowser.refresh();
    return;
  }
  submit_form(form_username, form_password, form_email, form_name, form_birthday);
}
```

## POSSIBLE QUESTIONS

## UNIT V

## PART-A (Online Examinations)

## PART-B (5 X 6 = 30 Marks)

**(Answer ALL the Questions)**

1. List out the functions in the WML libraries with examples for usage.
2. Write in detail about WML script.
3. Discuss in detail about user input operations in WML.
4. Explain in detail about functions in WML with example.
5. Discuss in detail about user input operations in WML.
6. Elaborate about functions in WML Libraries with example.
7. How does a WML application call a Perl script or ASP page? Explain.
8. Give the structure of table in WML and explain with example.
9. Explain in detail formatting output in WML.
10. Give the structure of table in WML and explain with example.

## PART-C (1 X 10 = 10 Marks)

1. How does a WML application call a Perl script or ASP page? Explain.
2. Discuss about mobile agent applications with neat diagram.
3. What are the key characteristics of mobile computing applications? Explain.
4. Explain (i) i-mode (ii) BREW
5. Elaborate the role of XML in wireless web through an example.
6. Discuss MANET with examples.

## KARPAGAM ACADEMY OF HIGHER EDUCATION
**Coimbatore - 641021.**
**(For the candidates admitted from 2019 onwards)**

**DEPARTMENT OF COMPUTER SCIENCE,CA & IT**

## WIRELESS AND MOBILE COMPUTING - 19CSP105A

**UNIT V :(Objective Type/Multiple choice Questions each Question carries one Mark )**

**PART-A (Online Examination)**

| S.NO | QUESTIONS | OPTION 1 | OPTION 2 | OPTION 3 | OPTION 4 | KEY |
|---|---|---|---|---|---|---|
| 1 | TCS BIN means | **Telephony Control Specification – Binary** | Telephony Control Specification – Basic | Telecommunication Control Specification – Binary | Tele Control Specification – Binary | **Telephony Control Specification – Binary** |
| 2 | PPP means | Private-to-Private Protocol | Peer-to-Point Protocol | Private-to-Public Protocol | **Point-to-Point Protocol** | **Point-to-Point Protocol** |
| 3 | SCO means | Simultaneous Connection Oriented | Sequence Connection Oriented | **Synchronous Connection Oriented** | None of these | **Synchronous Connection Oriented** |
| 4 | ACL means | **Asynchronous Connection Less** | Asynchronous Connection Level | Asynchronous Connection Link | None of these | **Asynchronous Connection Less** |
| 5 | LMP means | **Link Management Protocol** | Link Management Program | Level Management Protocol | None of these | **Link Management Protocol** |
| 6 | BTS means | Base Transceiver System | Basic Transceiver Station | **Base Transceiver Station** | Base Transmission Station | **Base Transceiver Station** |
| 7 | BS means | Base System | Basic Security | **Base Station** | Basic Station | **Base Station** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8 | MTSC means | Mobile Teleconferencing Service Center | **Mobile Telecommunication Service Center** | Mobile Telecommunication System Center | Mobile Telecommunication Security Center | **Mobile Telecommunication Service Center** |
| 9 | AOA means | Arrival of analog | **Angle of arrival** | Angle of access | Analog of arrival | **Angle of arrival** |
| 10 | SIM refers to | Supplier Identity Module | Subscriber Identity Method | Subscriber Identity Model | **Subscriber Identity Module** | **Subscriber Identity Module** |
| 11 | IMTS means | Improved Mobile Telephone Service | Improved Mobile Telephone Security | **Improved Mobile Telephone System** | Improved Mobile Telecommunication System | **Improved Mobile Telephone System** |
| 12 | AMPS means | **Advanced Mobile Phone Service** | Advanced Mobile Phone Security | Advanced Mobile Phone System | Advanced Mobile Protocol Service | **Advanced Mobile Phone Service** |
| 13 | GSM means | Good Service for Mobile Communication | **Global System for Mobile Communication** | Global System for Mobile Concepts | Global Service for Mobile Communication | **Global System for Mobile Communication** |
| 14 | MS means | Mobile Security | Mobile Service | Mobile System | **Mobile Station** | **Mobile Station** |
| 15 | CDPD means | Cellular Device Packet Data | Cellular Digital Packet Device | Cellular Data Packet Device | **Cellular Digital Packet Data** | **Cellular Digital Packet Data** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 16 | GPRS means | General Packet Radio Service | **Global Packet Radio Service** | Global Packet Recovery Service | Global Packet Radio System | **Global Packet Radio Service** |
| 17 | EDGE means | **Enhanced Data Rates for GSM Evaluation** | Enhanced Device Rates for GSM Evaluation | Extended Data Rates for GSM Evaluation | Enhanced Data Rates for Global system Evaluation | **Enhanced Data Rates for GSM Evaluation** |
| 18 | UMTS means | Mobile Telecommunications System | Universal Mobile Telecommunications Service | **Universal Mobile Telecommunications System** | Universal Mobile Tele System | **Universal Mobile Telecommunications System** |
| 19 | IETF means | **Internet Engineering Task Force** | Intranet Engineering Task Force | Both a and b | None of these | **Internet Engineering Task Force** |
| 20 | WS means | Wireless Services | Wireless System | **Web Services** | Web System | **Web Services** |
| 21 | VPN means | Virtual Private Netware | **Virtual Private Network** | Virtual Public Netware | Virtual Public Network | **Virtual Private Network** |
| 22 | VAN means | Value Added Netware | Voice Added Network | **Value Added Network** | None of these | **Value Added Network** |
| 23 | TMN means | **Telecommunications Managed Network** | Tele Managed Network | Telemedicine Managed Network | Telecommunications Metropolitan Network | **Telecommunications Managed Network** |
| 24 | SNA means | Security Network Architecture | **System Network Architecture** | System Netware Architecture | Service Network Architecture | **System Network Architecture** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 25 | PCS means | **Personal Communication System** | Communication System | Personal Communication Service | Personal Connectivity Service | **Personal Communication System** |
| 26 | QoS means | Quantity of Service | Quality of Security | **Quality of Service** | Quality of System | **Quality of Service** |
| 27 | NOS means | Quantity of Service | Quality of Security | **Network Operating Systems** | Netware Operating Systems | **Network Operating Systems** |
| 28 | NCP means | Network Control Process | Network Connectivity Program | **Network Control Program** | Netware Control Program | **Network Control Program** |
| 29 | MIPS refers to | **Million Instructions Per Second** | Mega Instructions Per Second | Million Instruments Per Second | None of these | **Million Instructions Per Second** |
| 30 | LU means | **Logical Unit** | Level Unit | Both a and b | None of these | **Logical Unit** |
| 31 | GUI means | Graphical User Interaction | Graphics User Interface | Graphical User Intra face | **None of these** | **None of these** |
| 32 | IEEE means | Institute of Electrical and Electronic Engineering | Institute of Electrics and Electronic Engineers | **Instituteof Electrical andElectronic engineers** | Information of Electrical and Electronic Engineers | **Instituteof Electrical andElectronic engineers** |
| 33 | IP means | **Internet Protocol** | Intranet Protocol | Interface Protocol | Internet Program | **Internet Protocol** |
| 34 | EB means | Electronic Bus | **Electronic Business** | Electric Bus | Electrical Business | **Electronic Business** |
| 35 | DS refers to | **Directory Service** | Directory Security | Directory System | Define Service | **Directory Service** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 36 | DCS means | **Digital Communication System** | Communication System | Digital Communication Service | Define Communication System | **Digital Communication System** |
| 37 | ATM means | Asynchronous Transfer Machine | Asynchronous Transmission Mode | **Asynchronous Transfer Mode** | Asynchronous Transaction Mode | **Asynchronous Transfer Mode** |
| 38 | DNA means | **Digital Network Architecture** | Digital Netware Architecture | Device Network Architecture | Device Netware Architecture | **Digital Network Architecture** |
| 39 | WBMPs refers to | **Wireless bitmaps** | Wireless bits | Wireless blocks | Wired bitmaps | **Wireless bitmaps** |
| 40 | Micro browser will automatically wrap the text to the next line when the text reaches the margin. Is it true? | No | May be | **Yes** | Not Known | **Yes** |
| 41 | <b> </b>tag is used in WML for | **Bold Text** | Italic Text | Both a and b | None of these | **Bold Text** |
| 42 | <u> </u>tag is used in WML for | Bold Text | Italic Text | **Underlined Text** | None of these | **Underlined Text** |
| 43 | Local source image means | resides within the Server’s RAM | resides within the phone’s RAM | Both a and b | **Image resides within the phone’s ROM** | **Image resides within the phone’s ROM** |
| 44 | WTAI means | Wired Telephony Application Interface | Wireless Telephone And Interface | **Wireless Telephony Application Interface** | None of these | **Wireless Telephony Application Interface** |
| 45 | You define a variable simply by assigning a value to the variable. Is it true? | No | May be | **Yes** | Not Known | **Yes** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 46 | How do you access the value stored in a WML variable? | #VariableName | @VariableName | %VariableName | **$VariableName** | **$VariableName** |
| 47 | How do you assign a value to a variable within a WML application? | <input> | <setvar> | **Both a and b** | None of these | **Both a and b** |
| 48 | How do you specify the default value for an input operation? | <value> tag | **<input> tag** | Both a and b | None of these | **<input> tag** |
| 49 | How can you limit the number of characters a user can input? | <input> tags max attribute | <input> tags length attribute | <input> tags value attribute | **<input> tags maxlength attribute** | **<input> tags maxlength attribute** |
| 50 | What is the purpose of the asterisk (*) in the format specification “*A”? | **User can enter any number of uppercase letters** | User can enter any number of lowercase letters | User can enter minimum number of uppercase letters | None of these | **User can enter any number of uppercase letters** |
| 51 | What is the purpose of the <select> tag’s multiple attribute? | **User selects multiple options** | User selects single option | User selects two options | None of these | **User selects multiple options** |
| 52 | What is a function? | **Small uniquely named piece of code** | Small multiple named piece of code | Both a and b | None of these | **Small uniquely named piece of code** |
| 53 | What is .wmls extension? | WML deck | **WMLScript functions** | Both a and b | None of these | **WMLScript functions** |
| 54 | Does WMLScript provide a run-time library? | **Yes** | Sometime | Both a and b | None of these | **Yes** |
| 55 | How do you create a comment within WMLScript? | Block Comment (/* */) | Two Slashes (//) | **Both a and b** | None of these | **Both a and b** |

| | | | | | | |
|---|---|---|---|---|---|---|
| 56 | What is a library? | Single Procedure | Mathematical Functions | Single function | **Collection of external functions** | **Collection of external functions** |
| 57 | What is a parameter? | **Value** | Variable | Both a and b | None of these | **Value** |
| 58 | Do all microbrowsers support the WMLScript Libraries? | Yes | **No** | Partially | None of these | **No** |
| 59 | How would you generate a random number in the range 0 to 5? | Pass the value 5 to Lang1 Library | Pass the value 5 to String Library | Both a and b | **Pass the value 5 to Lang Library** | **Pass the value 5 to Lang Library** |
| 60 | DML means | **Data Manipulation Language** | Data Markup Language | Both a and b | None of these | **Data Manipulation Language** |