Πανεπιστήμιο Μακεδονίας University of Macedonia
ΠΜΣ Πληροφοριακά Συστήματα Master Information Systems
Καθηγητές: Α.Α. Οικονομίδης & Α. Πομπόρτσης Professors: A.A. Economides & A. Pomportsis
Τεχνολογίες Τηλεπικοινωνιών & Δικτύων Networking Technologies

ΘΕΜΑ:

«Ασύρματα Δίκτυα - Wireless LANs»

Technology, Case Studies, Economics and Applications

ΜΑΡΙΑΝΘΗ ΤΕΡΨΙΑΔΟΥ

Α.Μ. 22106

MISO622

28 ΦΕΒΡΟΥΑΡΙΟΥ 2007

ΠΕΡΙΛΗΨΗ:

Οι ηλεκτρονικοί υπολογιστές καθώς και οι διάφορες ηλεκτρονικές συσκευές γίνονται ολοένα και περισσότερο δικτυωμένες τεχνολογίες με σκοπό την ευκολότερη πρόσβαση καθενός ενδιαφερόμενου σε κάθε είδους πληροφορία, ανά πάσα στιγμή και από οποιοδήποτε μέρος. Τα τελευταία χρόνια τα ασύρματα δίκτυα αποκτούν ολοένα και μεγαλύτερη φήμη λόγω του ότι παρέχουν φθηνή, φιλική προς τον χρήστη και αποτελεσματική πρόσβαση σε εφαρμογές που γίνονται περισσότερο φορητές.
Στην παρούσα εργασία κάνουμε μια εισαγωγή στην έννοια των τοπικών δικτύων, αναλύοντας τα ασύρματα τοπικά δίκτυα (WLANs)Παρουσιάζουμε την αρχιτεκτονική των ασύρματων δικτύων και των τοπικών δικτύων, τα πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία των WLANs, τα είδη των WLANs και τα πλεονεκτήματα και μειονεκτήματα που προκύπτουν από την χρήση τους. Παρατίθενται δύο χαρακτηριστικά παραδείγματα εφαρμογής των wireless τεχνολογιών (case studies) σε επιχειρήσεις / οργανισμούς. Εν κατακλείδι, παρουσιάζονται επιγραμματικά οικονομικά στοιχεία και το μέλλον των ασύρματων δικτύων.

SUMMARY:

Computers and microelectronic devices are increasingly being networked to bring to life anybody and anything, anytime, anywhere and to add value to devices by enabling them to access information and resources over any over any distance. In the last few years, WLANs have enjoyed enormous popularity for this purpose, because they provide user-friendly, inexpensive and effective access to applications that are becoming more portable.
In this project, we make an introduction in the significance of local networks, analyzing the wireless local networks (WLANs). We present the architecture of wireless networks and local networks, the protocols that are used for the communication of WLANs, the types of WLANs and the advantages and disadvantages that result from their use. There are mentioned two characteristics examples of application of wireless technologies (case studies) in enterprises/organisms. In conclusion, are presented succinct economic elements and the future of wireless networks.

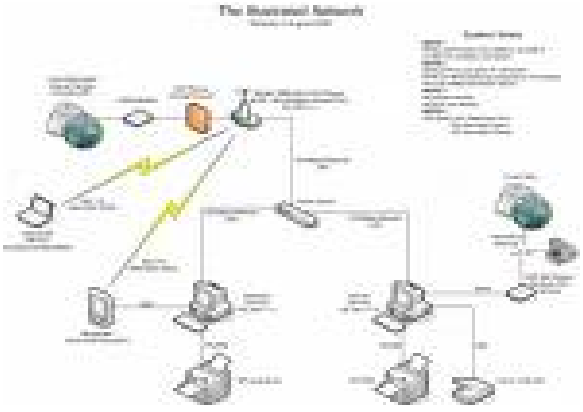
ΠΕΡΙΕΧΟΜΕΝΑ – CONTENTS :

ΜΟΝΑΔΑ

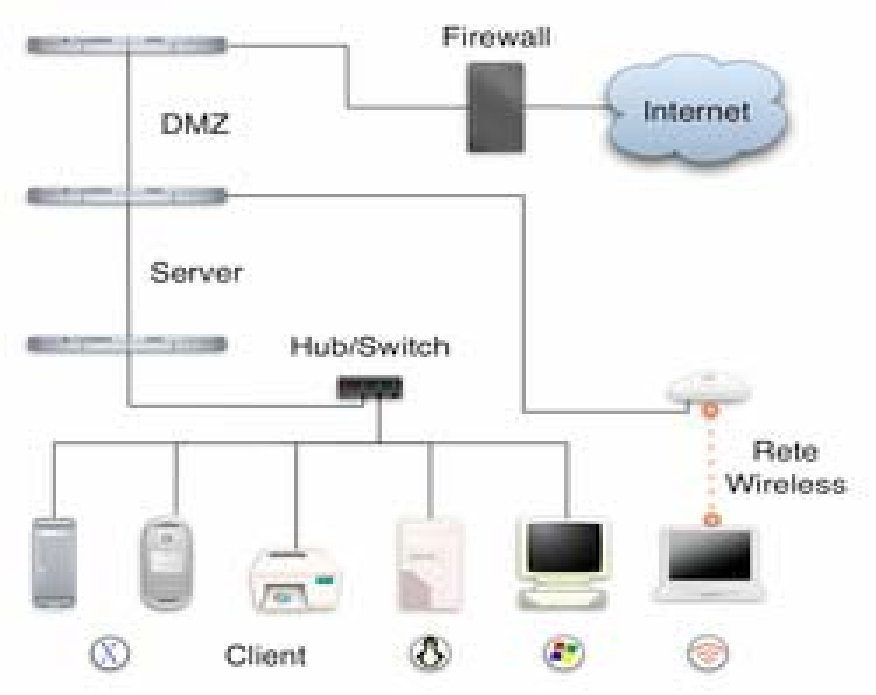
INTRODUCTION

-WHAT IS A LOCAL AREA NETWORK (LAN)?

A local area network is a computer network covering a local area like a home office, or a group of buildings .Involves the connection of several devices in the same area of a building .A typical scenario is the linking together of a client PCs servers and peripheral devices such as printers in an office .The typical distances between these devices may be a few ten or hundreds of metres. The first LANs were created in the late 1970s and used to create high-speed links between several large central computers at one site .Of many competing systems created at this time, Ethernet and ARCNET were the most popular. Current LANS are most likely to be based on switched IEEE 802.3 Ethernet technology , running at 10,100 or 1,000 Mbits , or on Wi-Fi technology. The characteristics of LANs are: high data rates , small geographic range , no leased telecommunication lines . There are two types of LAN: wired and wireless network .



HOME LAN 1



-ABOUT WIRELESS NETWORK:

In 1896 , Marconi Guglielmo began working with radio waves and established the Wireless Telegraph and signal company , the first radio factory in the world. By 1901 the first signals were being sent across the Atlantic Ocean. In 1971 , researchers at the University of Hawaii developed the world's first WLAN ,it was named ALOHAnet. The world is going wireless . The prohibitive cost of building wired network infrastructures has paved the way for wireless networking on a global scale. Developing countries , with more sophisticated network and Internet access than ever before, have surged ahead in the utilization of wireless networks so that even the most remote parts of the globe have coverage undreamed of only a few years ago .
Different types of wireless network are: a WIRELESS LAN ,GSM ,PCS ,D-AMPS ,Wi-Fi ,FIXED WIRELESS DATA .

-WHAT IS A WIRELESS LAN?

A Wireless LAN is a wireless local area network , which is the linking of two or more computers using wires .This standardized network technology that implements LAN functionality by using wireless data transfer .Furthermore, primarily includes the broadband connection of microelectronic devices in a range of ten metres to a hundred . It uses high-frequency radio waves rather than wires to communicate between nodes , in order to transmit data back and forth on the same network . Users have the mobility to move around within a broad coverage area and still be connected to the network .This technology is becoming more and more popular due to the rapid emergence of small portable devices such as PDAs. For the business , such as coffee shops or malls , have begun to offer wireless access to their customers , some are even provided as a free service. For the home user, wireless has become popular because of the ease of installation and location freedom with the gaining popularity of laptops. Most wlans operate over unlicensed frequencies at near-ethernet speeds using carrier sense protocols to share a radio wave or infrared light medium . Also , most wireless lan products offer Simple Network Management Protocols (SNMP)to support network management through the use of SNMP-based management platforms and applications.When you define your WLAN architecture, focus on two distinct technology alignment challenges:

- Alignment with business requirements
- Alignment with user requirements

To support the business, the WLAN architecture should facilitate and support the generation of a net positive value in the form of strategic, operational, or technological benefits. To effectively support the user, the architecture needs to take into account parameters such as usability, convenience, access, availability, and support. If the WLAN is not easy to use, is subject to poor coverage or uptime, or has little user support, the total WLAN experience will not be positive, resulting in little or no use of the infrastructure investment.

-ARCHITECTURE OF A WIRELESS NETWORK:

Network architecture, whether wireless or wired, may be viewed in two ways, physically and logically.

- -PHYSICAL architecture of WLANs:

The following sections explain the various components of a wireless LAN:

- End –User Appliances is an interface between the user and the network such as the following devices: desktop workstations, Laptop , Palmtop ,handheld Pushpin-based computers , PDA, Handheld scanners and data collectors , handheld printers
- Antenna radiates the modulated signal through the air so that the destination can receive it . Antennas come in many shapes and sizes and have the following specific electrical characteristics: propagation pattern, gain, transmits power, bandwidth.
- Communication Channel. Wireless networks use the air as the medium.
- Network software
- Wireless network Interface

- -LOGICAL architecture of WLANs:

Defines the network's protocols which ensures a well-managed And effective means of communication. PCs, servers, routers and other active devices must conform to very strict rules to facilitate the proper coordination and transfer of information. The seven layer Open System Interconnect (OSI) Reference model developed by ISO is one popular standard logical architecture.

-COMMUNICATION PROTOCOLS:

A communication protocol operates at a higher level and establishes end-to-end connections between the application software and within devices on the network. This is necessary to provide a common path for entities to communicate. The most common protocol for providing communications among network devices and applications are the Transmission Control Protocol (TCP) and Internet Protocol (IP). These protocols are the basis of standards for connecting to the Internet and providing open systems connectivity in other systems. TCP operates at the OSI Transport Layer and is commonly used for establishing and maintaining communications between applications on different computers. Also, it provides highly reliable, full-duplex, connection-oriented, acknowledged and flow-control services to upper-layer protocols and applications. The fields of a TCP datagram, which provide necessary functionality for reliable communications between a source and destination network device, are:

1. Source Port and Destination Port: identifies the service access points at which upper-layer source and destination processes and applications receive TCP services.
2. Sequence Number: specifies the sequence number of the datagram being sent.
3. Acknowledgement Number: contains the sequence number of the next datagram the sender of the immediate packet expects to receive.
4. Header Information: carries information about the TCP header.
5. Window: specifies the size of the sender's receiving window.
6. Checksum: determines whether the header contains errors.
7. Urgent Pointer: points to the first data in the packet byte that the sender wanted to mark as urgent.
8. Options: specifies various TCP options.
9. Data: contains upper-layer information and control data.

The IP operates at the OSI Network Layer. Routers commonly use IP to route TCP datagram's from source to destination. The fields of an IP packet, which provide functionality for routing across dissimilar networks, are:

1. Version: The version number of the IP.
2. Internet Header Length: The length of the IP header in 32 bit words.
3. Type of service: The level of service the IP datagram should be given an it traverses the network.
4. Total length: the length of the datagram in bytes.
5. Identification: Number of the datagram for combining datagram fragments.
6. Flags: Data bits for controlling whether fragmentation should take place.
7. Fragment Offset: The location of a datagram.
8. Time-to-Live: The maximum amount of time the datagram can exist.
9. Protocol: The protocol that associates with the data in the Data field of the datagram.
10. Header Checksum: 16-bit checksum of the datagram header.
11. Source IP Address: The IP address of the sender of the datagram.
12. Destination IP Address: The IP address of the destination of the datagram.
13. Options: A set of fields that describe specific processing that must take place on the packet, especially used for debugging and testing.
14. Padding: Additional data bits to ensure the packet is a complete set of 32 bit words.

-IEEE 802.11 MAC PROTOCOL:

In Wireless LAN the medium access protocol (MAC) is the main element for determining the efficiency in sharing the limited communication bandwidth of the wireless channel. The transmissions of the network stations must be coordinated by the MAC protocol. The IEEE802.11 MAC protocol provides asynchronous, time-bounded and contention free access control on a variety of physical layers. The MAC layer service provides the capability for peer LLC entities to exchange MAC service data units (MSDUs) between MAC service access points (SAPs). The MAC Layer provides these primary operations:

- ✓ Accessing the wireless medium

The basic access method in the 802.11 MAC protocol is a Distributed Coordination Function (DCF) which is a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) MAC protocol.

- Multiple Access (MA) means that several communications participants can use the same transmission channel(shared medium).

- Carrier Sense(CS) means that each communications participant can monitor the same channel and adjust their own activity to match the channel's state. In particular no station can start transmitting if it detects that the channel is busy. The IEEE802.11 standard differentiates between physical listening which uses the measured field strength to evaluate a channel's activity, and virtual listening . A station can use a special protocol to reserve a specific channel for a particular time interval.

- Collision Avoidance (CA) describes the algorithms used to prevent collisions on the channel.

Another basic access mechanism is the Point Coordination Function (PCF) which is similar to a polling system and uses a point coordinator to determine which station has the right to transmit.

Although PCF is optional, all stations must be capable of using the PCF sequence media access rules, firstly because these are based on DCF and secondly because , if they did not , this principle would have no effect. PCF controls a frame's transfer during a Contention Free Period (CFP) which alternates with DCF –controlled Contention Periods (CP).

- ✓ Joining a network

After a station is turned on, it needs to first determine another station or access point present to join before authenticating and associating with an applicable station or access point. The station accomplishes this discovery phase by operating in a passive or active scanning mode. After joining with a BSS or a ESS , the station accepts the Service Set Identifier (SSID), Timing Synchronization Function (TSF), timer value, and PHY setup parameters from the access point.

- ✓ Providing Authentication and Privacy

The 802.11 standard describes two following types of authentication services that increase the security of 802.11 networks:

1. Open system authentication: The default authentication service that just announces the desire to associate with another station or access point.
2. Shared key authentication: Involves a more rigorous exchange of frames, ensuring the requesting station is authentic.

In an effort to increase throughput, IEEE established two task groups to explore alternate implementations of 802.11. Task Group A explored the 5-GHz band, both to produce low –cost equipment operating at such high frequencies and to reconcile competing international uses of this spectrum, may keep their 802.11a standard from reaching wide distribution . Task Group B explored more sophisticated spectrum spreading technologies in the original 2.4 GHz band. 802.11b specifies the lowest layer of OSI model (physical) and a part of the next higher layer . The majority of wireless lans in the market follow the 802.11b standard. In addition, the standard

specifies the use of the 802.2 protocol for the logical link control portion of the data link layer.

- **Extensions to IEEE802.11 standard:**

802.11a	Definition of a PHY using an OFDM modulation process with 10 carrier frequencies at 5GHz and data rates up to 54 Mbps.
802.11b	Definition of a PHY using a DSSS modulation process with 10 carrier frequencies at 2.4GHz and data rates of up to 11 Mbps.
802.11b-cor1	Connections to management information base in 802.11
802.11-c	Addition of specific MAC procedure IEEE802.11, to enable 802.1-compitable bridging functionality.
802.11-d	Extension of PHY definitions to apply to new countries.
802.11-e	Improvements in service support for transfer effiency in the Distributed Coordination Function and Point Coordination Function, as well as for security mechanisms.
802.11-f	Internet Access Point Protocol for roaming and Load Balancing.
802.11-g	Extension to the 802.11b standard for 22Mbps.
802.11-h	Extension of the 802.11 MAC protocol and the 802.11 a PHY protocol in the 5GHz range
802.11-i	Extension of the MAC protocol to improve security and authentication mechanisms.

-BLUETOOTH COMMUNICATION PROTOCOL:

The Bluetooth standard is based on three application scenarios which position it at Personal Area Networks level:

- Replacing cables
- Data and voice access points
- Personal ad hoc networks

To provide these applications you do not necessarily need PCs. Often it is the case that relatively cheap and simple devices with a wireless connection can be used. For this reason Bluetooth standards needs to allow the simplest and cheapest solutions possible. The description of the Bluetooth communications protocols includes all the levels of the protocol layers. Provides a complete radio system. Most important elements of the Bluetooth standard:

- RF and baseband
- Link Manager Protocol(LMP) , responsible for network management tasks.
- Logical Link Control and Adaption Protocol(L2CAP), connects the protocols of the higher layers with the tasks of the baseband.
- Service Discovery Protocol(SDP), recognises different services and the characteristics of each service.
- Wireless Cable(RFCOMM), describes a point-to-point connection between two devices over the “air serial port”.
- Telephone coupling

Types of Bluetooth:

A Bluetooth network essentially uses a master/slave architecture in which the master controls the traffic flow. There exist 2 types of Bluetooth network:

1. Pico network, when one master is present in a network
    i. Mono-slave mode: point-to-point connection
    ii. Multi-slave mode: point-to-multipoint connections
2. Scattered pico networks, consist a scatternet, where there are several masters in scatternet mode.

-DECT COMMUNICATION PROTOCOL :

The DECT standard is designed to handle a point-to-point connection between a base station, the Fixed Part (FP) and a mobile device, the Portable Part (PP). A Base station can process the traffic between several mobile devices and the fixed network, or also the mobile devices can do so themselves. In addition, several base stations can be interconnected to allow roaming and handover.
An MC/TDMA/TDD algorithm is used to distribute the frequencies for the various channels within this frequency band. DECT works in a reserved frequency area which, in Europe, lies between 2.88 and 2.9 GHz. On other continents other frequency ranges of 2.5 to 3.6 GHz are used. The technologies used in these hogher frequency areas are called Upbanded DECT.

-HomeRF PROTOCOL :

As its name suggests, it is primarily intended for networking private households. The 2.0 version also addresses small company networks :supports fast speeds and movement of stations between cells.
In HomeRF terminology, stations that act as data sources or recipients are called nodes. HomeRF networks permit the same network architecture as 802.12. This means there is support both for communication between nodes and communication between a central point, called connection point (CP) and several nodes. In addition , HomeRF version 2.0 onward also supports roaming nodes from the cell of one central point to the cell of a different central point.

Classes of nodes :

- -asynchronous nodes (A-Node)
- -synchronous nodes (S-Node)
- -isochronous nodes (I-Node)

-HiperLAN/2 PROTOCOL :

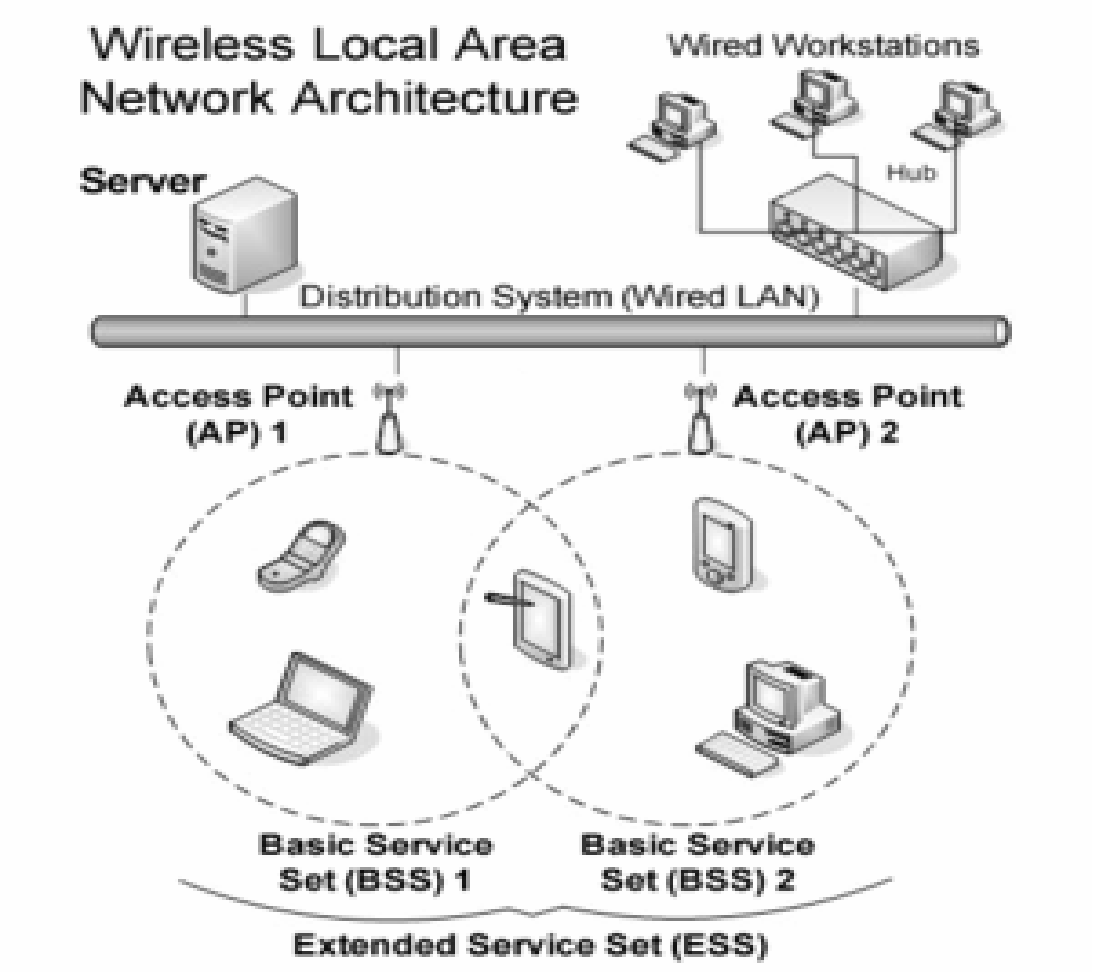
It has been extended with two new components: the HiperACCESS and the HiperLINK. The HiperACCESS protocol has a point-to-multipoint architecture, and is designed to offer access for residential areas and business customers for ranges of up to 5 km. HiperLINK is used for point-to-point links with very high data rates of up to 155 Mbps over distances of up to 150m. In particular it supports HiperLAN/2 and HiperACCESS interconnections over short routes. A HiperLAN/2 network consists of several Access Points. They provide radio coverage in a particular geographical area, called a cell. In these cells the mobile participants, known as Mobile Terminals communicate with these points.
In the area of 5 GHz there are two competing technologies, the HiperLAN/2 standard and the IEEE802.11a. Although they are more or less identical at the level of physical transfer they differ at the level of channel access. From the technical point of view the HiperLAN /2 standard seems superior, but to succeed in the market place, other political and company-related aspects and cost issues are important.

-ARCHITECTURE OF WIRELESS LAN

All components that can connect into a wireless medium in a network are referred to as stations . The components of a wireless lan consist of a wireless NIC (network interface card) and a wireless local bridge which is often referred to as an access point . The wireless NIC interfaces the appliance with the wireless network and the access point interfaces the wireless with a wired network. Most wireless NICs

interfaces appliances to the wireless network by implementing a carrier sense protocol and modulating the data signal with a spreading sequence.
STATIONS fall into one of two categories: Wireless Clients and Access Points.

- Access Points are base stations which transmit and receive radio frequencies for wireless enabled devices to communicate with .
- Wireless clients can be mobile devices such as laptops, PDAs, IP phones or desktops and workstations that are equipped with a wireless network interface card .



DISTRIBUTION SYSTEM : connects Access Points in an extended service set.

BASIC SERVICE SET (BSS): is a set of all stations that can communicate with each other . Every BS$$S has an id called the BSSID. There are two types of BSS:

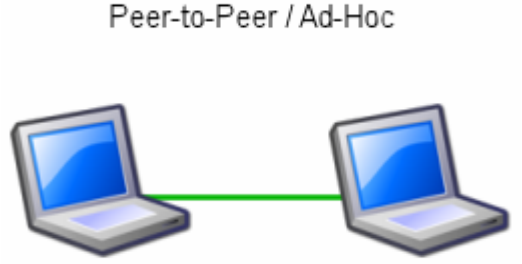
1. Independent BSS: are an ad-hoc network that contain no Access Points so they can not connect to any other basic service set.
2. Infrastructure BSS:can communicate with other stations not in the same basic service set by communicating through access points.

EXTENDED SERVICE SET (ESS): is a set of connected BSS which has an 32 byte character string id called SSID .

-TYPES OF WLANs:

- Peer -to –Peer or ad-hoc :

This type allows wireless devices to communicate each other directly, typically used by two computers. Wireless devices within range of each other can discover and communicate directly without involving central access points.



- Wireless distribution system :

Put up access points as repeaters

- Monitoring station :

Wireless network cards can be set up to monitor a network without connecting to an access point or revealing itself. This can be used for NIDS, diagnostics and troubleshooting to sniff clear-text activity or crack encryption.

-ADVANTAGES OF WIRELESS LANS:

The emergence and continual growth of wireless lans are being driven by the need to lower the cost associated with network infrastructures and to support mobile networking applications that offer gains in process efficiency , accuracy and lower business costs. The majority of computers sold to consumers today come pre-equipped with all necessary wireless LAN technology. Due to the numerous portable and pocketable devices used for voice and data processing or data transfer via wireless transmission , WLANs can replace the corresponding cabled solutions on the same network level. Problems with incompatible connectors (plugs) or missing cables can become a thing of the past. The benefits include:

1. Mobility : enables users to move while using an appliance.
2. Cost Savings : Because of the lack of a tether between the user's appliances and a server , wireless networks offer benefits that reduce costs.
3. Convenience : allows users to access network resources from nearly any convenient location within their primary networking environment.
4. Productivity : Users can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.
5. Deployment : Initial setup of an infrastructure-based wireless network requires little more than a single access point.
6. Expandability: Wireless networks can serve a suddenly-increased number of clients with the existing equipment.
7. Long-term cost savings : Changes and renovations In a business requires huge amounts of money.

-DISADVANTAGES OF WIRELESS LANS:

The advantages described above are certainly welcomed by companies and organizations, however, wireless LANs may not be

desirable for many reasons. Network managers and engineers should be aware of the following concerns that surround the implementation and use of wireless lans:

1. Radio Signal Interference: The process of transmitting and receiving radio and laser signals through the air makes wireless systems vulnerable to atmospheric noise and transmissions from other systems. Interference can take on an inward or an outward direction.

2. Range: The typical range of a common 802.11g network with standard equipment is o the order of ten meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly.

3. Security: Are wireless LAN secure? To answer this question you must consider the functionality of a wireless network performs. Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Furthermore, due to the space and cost, the 'antennas' are nothing more than the most naive of reception devices. Radio waves easily penetrate building walls and are receivable from the facility's parking lot and possibly a few blocks away. Someone can retrieve your company's sensitive information by using the same wireless NIC from this distance without being noticed by network security personnel. This requires that the intruder obtain the network access code necessary to join the network. This problem also exists with wired networks but to a lesser degree. Another security problem is the potential for electronic sabotage, in which someone maliciously jam the radio-based network and keeps you from using the network.

4. Connection Problems : TCP/IP is susceptible to losing connections especially when the appliance is operating in an area with marginal wireless network coverage. Also the mobile nature of wireless lans can offer addressing problems. Most networks require IP address loaded in the user's appliance to be within a specific address range to maintain proper connections with applications. When a user roams with a wireless appliance from one IP subnet to another , the appliance and the application may lose the capability to connect with each other.

5. Speed : The speed on most wireless networks(1-54 Mbps) is far slower than even the slowest common wired networks(100Mbps up to several Gbps). However, for most users ,this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. In most environments your wireless network running at its slowest speed is still dozens of times faster than the DSL serving it in the first place.

-Techniques for dealing with :

Interference: you should coordinate the operation of radio-based wireless network products with your company's frequency management organization , if on exists. Government organizations and most Hospitals have people who manage the use of transmitting devices. This coordination will avoid potential interference problems.

Security Safeguards: requires most products to establish a network access code and set the code within each workstation. A wireless station will not process the data unless its code is set to the same number as the network.

-WIRELESS NETWORK MARKETS AND APPLICATIONS :

Wireless networking is applicable to all industries with a need for mobile computer usage or when the installation of physical media is not feasible. Such networking is useful when employees must process information on the spot, directly in front of customers, via electronic-based forms and interactive menus. Wireless LANs makes it possible to place portable computers in the hands of mobile frontline workers such as doctors, nurses, warehouse clerks, inspectors, claims adjusters, real estate agents and insurance salespeople. The coupling of portable devices with wireless connectivity to a common database and specific applications, meets mobility needs, eliminates paperwork, decreases errors, reduces

process costs and improves efficiency. Retail organizations need to order , price ,sell and keep inventories of merchandise and sales people are equipped with a pen-based computer or a small computing device with bar code reading and printing capability, with the wireless link to the store's database.
Warehouse staff must manage the receiving, putting away, inventory and picking of goods. Each warehouse employee
has a handheld computing device with a bar code scanner interfaced via a wireless network to a warehouse inventory system. Health care centers must maintain accurate records to ensure effective patient care. The use of mobile electronic patient records is possible by providing each nurse and doctor with a wireless pen-based computer, coupled with a wireless network to databases that store critical medical information about the patients. Also, the use of handheld bar code printing and scanning devices dramatically increases the efficiency and accuracy of all drug transactions. Most importantly, however, it ensures that hospital staff can administer the right drug to the right person in time. Hospitality establishments check customers in and out and keep track of needs such as room service orders and laundry requests. Wireless computers are very useful in the situations where there is a large crowd, such as a restaurant. Utility companies employ wireless networks to support the automation of meter reading and system monitoring, saving time and reducing overhead costs. A field service employee can carry a portable computer connected via a wireless network to the office LAN containing accurate documentation of all applicable information. With wireless access to the home office

network, a salesperson can view centralized contact information, retrieve product information, produce proposals, create contracts and stay in touch with home office staff and other salespeople. Finally, a wireless LAN can support the monitoring of stock levels by transporting applicable data from each of the vending machines to a central database that can be easily viewed by company personnel from a single location.

CASE STUDY ONE: GENERAL CAMPUS WIRELESS NETWORK

At this institution, 40 wireless access points have been installed across the main campus. They are from the same manufacturer, use 802.11b and are connected as a single, virtual network to a gateway which requires a username and password. The access points provide wireless coverage for most recreational and social spaces on campus, such as bars and refectories. It also covers parts of the Library and some outdoor spaces where students gather.

The wireless network is predominantly used by students, although there are some staff users. Students supply their own wireless cards, although most are now using laptops with them built in, and there have been few problems with configuring their cards. There are about 200 users who have used the wireless network and email and web browsing are the most popular applications. There are a very small number of PDA users who are also using the wireless network to access their email.

The wireless network was installed during the Michaelmas term 2001 and was very lightly used for the first year. The number of users has grown significantly since that time and is expected to continue to grow. The performance of the network is generally quite good in areas where the signal is strong and the large number of access

points means that there are only a few active users on each. The nature of email and web page network traffic means that each user generates short bursts of network activity which works quite well with this technology.

Prior to the installation of the gateway, security was a major concern and there was some evidence of unauthorised people using the wireless network. Maintenance of the access points is fairly labour intensive and it is generally necessary for the administrator to manually change configuration settings or upgrade the firmware on each access point individually. Where an area receives a signal from more than one access point and both are using the default channel, users can experience interference and consequently very poor performance. To address this problem, a survey of the signals across the campus will be conducted and specific channels assigned to each access point so that there are no longer any overlapping signals on the same channels.

This example demonstrates the strengths and value of a campus wireless network. It has sufficient access points, is being used for applications that generate bursts of activity and so are suited to a shared network and is secured against extraneous use. The security and channel interference issues do however demonstrate the importance of pre-installation planning.

CASE STUDY TWO: ODD & CIE ADOPT THE WLAN TECHNOLOGY

- **Going wireless reaps rewards for investment company**

Oddo&Cie is France's leading independent investment company, run and owned by family and partners. It offers a range of services and products to institutional and private investors and companies in France and elsewhere. The company has a staff of 642 and 176 million € in consolidated shareholders' equity. It has 8.8 billion € in assets under management and 85 mutual funds. Oddo&Cie's 40-strong research team produces 7,000 pages of research a year and is one of the most renowned in Paris. It is the engine that drives all the company's brokerage-related services while providing

information, analysis and recommendations to the company's other departments. Oddo&Cie is based in a nineteenth century listed building in the heart of Paris. Of its seven floors, two are under ground and the foundations are 28 inches thick. This created significant challenges when the company needed to upgrade its whole wired infrastructure from 5-cat to 6e-cat.

The 5-cat infrastructure was getting old, but being in a listed building meant Oddo&Cie was severely constrained in what it was allowed to do to the walls, floors and ceilings. The thickness

Of the walls and foundations presented a further obstacle. Olivier Huynh Van, Networks & Systems Manager at Oddo&Cie, says: "We needed to get rid of the old cable system and wanted a completely new solution with network connections in some of the oldest rooms including the appointment rooms where customers are received." These rooms are used for presentations, demonstrations and customer meetings. But because the building is a listed landmark, skilled workmen and specialized architects would be needed to do any modifications to the old rooms. The process would have been long, complex, bureaucratic and expensive. "We needed an economic solution and we needed it quickly,". "The WLAN network topology cost lest than two per cent of the cabling project," Huynh Van says. WLAN technology also meant it was possible to hide the hot spots and conform to architectural regulations for listed buildings. Unsightly wiring and boxes can be avoided because the access points and antennae are hidden in the walls. Security would also be much greater because the lack of wires or sockets on the walls or the floor means that guests cannot access the network physically. "There is no risk of an authorized person accidentally leaving an opening for someone to access critical data," Huynh Van says. Use of client based VPN access in conjunction with a WLAN for staff when on the move would ensure the tight security conditions would apply to anyone trying to use the corporate network worldwide. The client-based approach provides an additional level of encryption above the standard Wireless Encryption Privacy (WEP) for WLAN. This prevents data theft from eavesdropping between the mobile device and the VPN firewall.

The VPN Mobile-Units facility allows staff on the streets to access their data from anywhere through a regular Internet access (via xDSL, cable, PSTN, GPRS or another service). The remote host establishes an encrypted link over the public network. On the other

side, mobile users inside the company use the WLAN Mobile- Units facility. Both facilities feature IPSec tunnel and user authentication. The client-based VPN approach ensures the highest possible levels of security and prevents data theft from eavesdropping between the mobile device and VPN firewall.

The WLAN is behind firewalls with two access levels: guest level and colleague level. Guest level uses the standard WEP system for WLANs, while colleague level employs ultra secure encryption between the mobile device and the firewall.

Productivity gains

The WiFi system has delivered significant productivity gains for the network team and the security team at Oddo. “With a wired system there is lots of tracking work to be done shutting down ports and removing cables when consultants move, and opening them for new people,” Huynh Van says. “With a wireless system this doesn’t need to be done, saving hours of technical support time.”

A welcome feature of the system is the ability to manage all access points together, for example adding new MAC addresses to each one simultaneously or flashing all hot spots with new firmware. Oddo also likes the fact that Intel continues to upgrade and enhance its products. “The firmware embedded on the access points is always improving,” says Huynh Van. “Moreover, lots of the enhancements are free and can simply be downloaded from Intel’s Web site. So you can benefit from a new feature immediately.”

Firewall protection

Given the nature of the investment business, Oddo needed the highest levels of security for its new system. This was not a problem with the WLAN. On the contrary, the wireless service enables Oddo to build in stronger and safer security\ than was previously available under the hardwired system. The system has also delivered a higher level of management control.

Flexibility, reliability and price performance

The decision to go with WLAN has proved the right one at Oddo&Cie, and the company is delighted with its Intel-based network. “The reason for choosing Intel was because of the maturity of its offering, the fact that it had a solution whether we wanted connectivity from desk top to notebook or palm top,” Huynh Van says. “After evaluation and implementation we are totally satisfied with the results we have had from Intel products.”

The fact that the wireless products featured enough flexibility to provide network connectivity in the whole building with a minimum investment – less than two per cent of the cabling project budget – further underlines the enormous advantages of the WLAN solution.

The future

Oddo&Cie aims to implement the WLAN technology at its other buildings in Paris at some point in the future. Even though these buildings have none of the architectural constraints of the head office, the benefits of the WLAN solution from a cost, convenience and security point of view make it ideal for further deployment when economic conditions allow. Another benefit expected over the next six months to two years is increased productivity among Oddo's staff. Regulatory issues have held back the spread of WLAN systems in France so that people are relatively unfamiliar with its potential to improve personal productivity. "At present, many people are still using the wireless technology in the same way as they use their desktop systems," says Huynh Van. "However, as hot spots and wireless systems become more widespread in France, we anticipate that employees will begin to adapt their working practices to exploit the productivity benefits of WLAN technology."

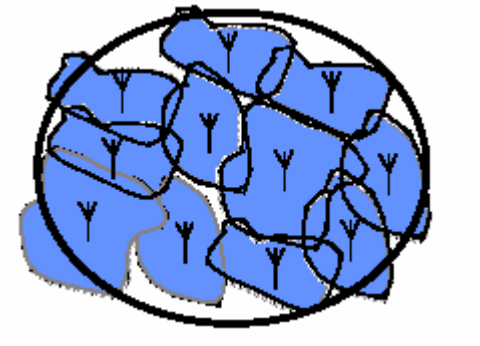
- ✓ Our conclusions, over the above statements, could say that WLAN technology offers enormous cost-savings over a conventional hard-wired network solution. In the case of the Oddo & Cie network, the price came down remarkably to less than two per cent of the cost of cabling the building. The WLAN is also cheaper to maintain thanks to productivity gains in technical support. Where the fabric of a building is particularly historic or architecturally interesting and needs to be maintained, WLAN technology provides the potential to install a fully-functional state of- the-art communications network without causing damage or introducing unsightly wires and sockets. Security can be significantly increased with WLAN by avoiding the need for sockets that might enable unauthorised access. WLAN also prevents the possibility of ports being accidentally left open for intruders to penetrate. Using a WLAN in combination with a client-based VPN also enhances global security. Flexibility and versatility are key features of a WLAN, enabling users to work at a time and

place that suits them and access all the corporate data they need and are authorised to obtain. Offers such a broad range of WLAN components that it is possible to set up the entire network and obtain adapters, drivers and other key components to run the complete system using Intel technology.

-ECONOMICS OF BROADBAND WIRELESS ACCESS:

•Economic success of mobile telephony industry as we know it does not scale in terms of bandwidth
–The same users have to pay for more infrastructure
•Shared wide-area “anywhere, anytime” infrastructure deployment very slow despite of rapid advances in IT
–Moore’s law applies to electronic equipment -not infrastructure

- Key problems in Wireless Systems:

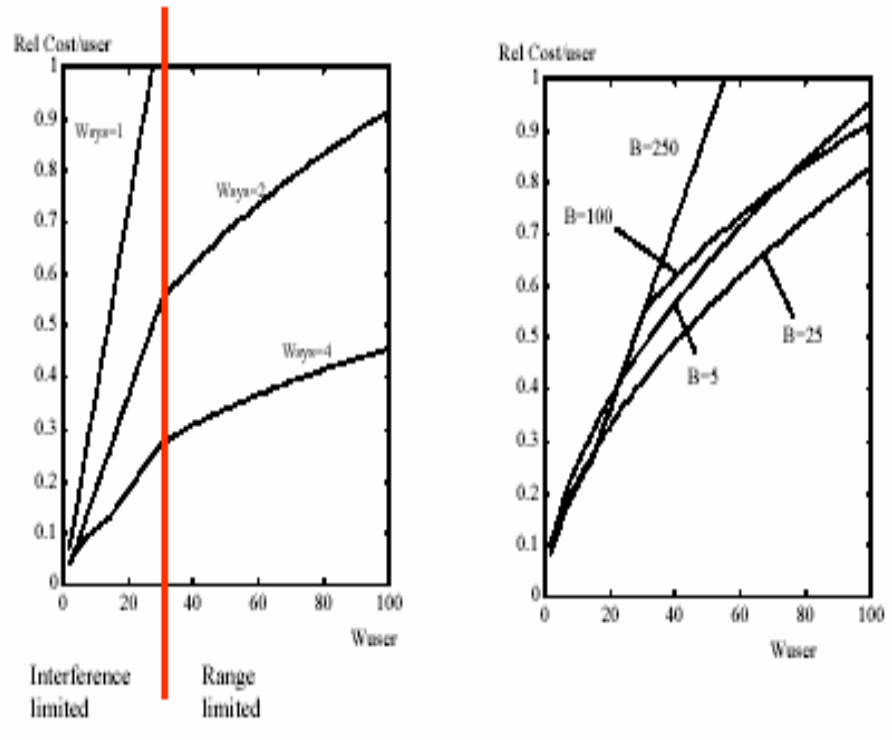


- Wireless system

-Infrastructure
  - Base stations (RAPs)
  - Fixed network

-Terminals
- Coverage requirements
- Service requirements

- Some simple Infrastructure Cost Models:



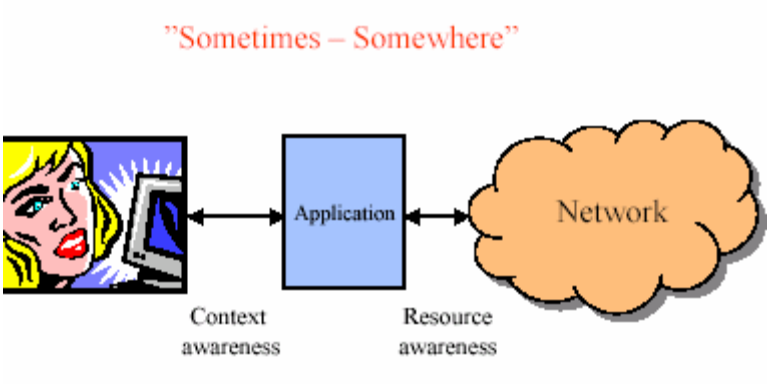
Cost/Bandwidth example 1

- Breaking the cost barrier :

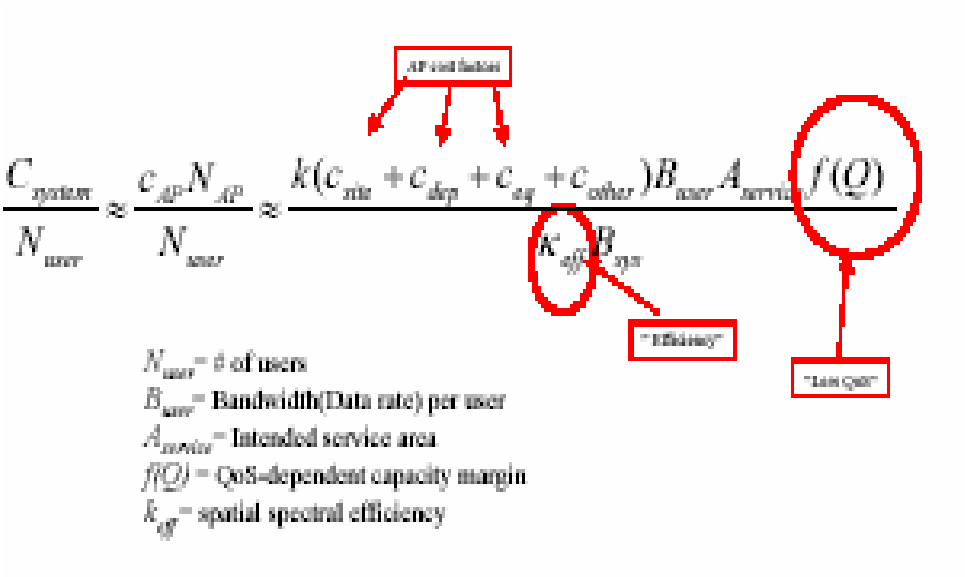
$$C_{system} = cN_{user}B_{user}A_{service}f(Q)$$

•Sacrifice bandwidth/compatibility ? (Lower B)
•Sacrifice uniform coverage (Lower A)
•Sacrifice QoS guarantees (Lower f(Q) -delay, availability..)

- Surviving without QoS guarantees:



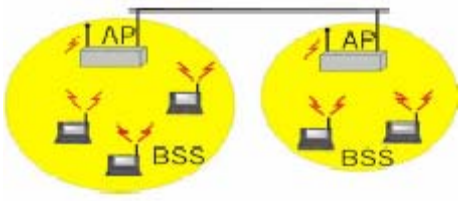
- Affordable Wireless Systems?



- Affordability- some key questions to be addressed in

  - ❖ More affordable –not necessary higher performance in traditional sense (e.g. higher bit rates,…)
  - ❖ What are the cost factors that are
    - significant
    - can be influenced by (our) technology?

- Distributed systems :
  -Low cost-high speed access
  -User-deployed
  -Self-organizing , organic growthm
  -10-5- Mbits/s
- Partial and sporadic coverage
  10-50 m
- Dynamic sharing of the unlicensed spectrum with almost no QoS guarantess
- No mobility management
- No charging mechanisms
- The true “Wireless Internet”



-THE FUTURE OF WIRELESS LANs:

Where is the wireless networking going? What will the future bring? The outlook of wireless LANs is very good. The production of new wireless products will drive the prices down. The presence of standards will motivate smaller companies to manufacture wireless components because they will not need to invest large sums of money in the research and development phases of the product, These investments already will have been made and embodied within the standards, which will be available to anyone interested in building wireless network components.

Bibliography- Βιβλιογραφία:

1. Δίκτυα Υπολογιστών , εκδόσεις Κλειδάριθμος, συγγραφέας Tanenbaum
2. Wireless Personal and Local area networks, εκδόσεις Wiley , συγγραφέας Axel Sikora
3. Wireless Lans, εκδόσεις Macmillan Technical Publishing USA, συγγραφέας Jim Geier
4. Στοιχεία από Wikipedia, the free encyclopedia για WIRELESS LAN, WIRELESS NETWORK.
5. Δικτυακοί τόποι : www.bluetooth.gr , www.dect.gr , www.wireless-nets.com
6. Στοιχεία από www.google.gr για τα ασύρματα δίκτυα, Analyzing and Improving the IEEE802.11 MAC Protocol,