Wireless Technology

Rajiv Puri
AVP - Operations
Houston
Technologies Ltd.

Agenda

- Houston Technologies Limited
- Wireless Technologies
- Bluetooth – Uses, security
- WLANs – Challenges, security
- WiMax
- Wireless WAN

Houston Technologies Limited

Splendor House
F-38/2, Okhla Industrial Area, Phase II,
New Delhi – 110 020, India
Phone: +91-11-26383002/07
Fax: +91-11-26383225

Website: **www.houstontechnologies.com**
email: **contact@houstontechnologies.com**

ABOUT US

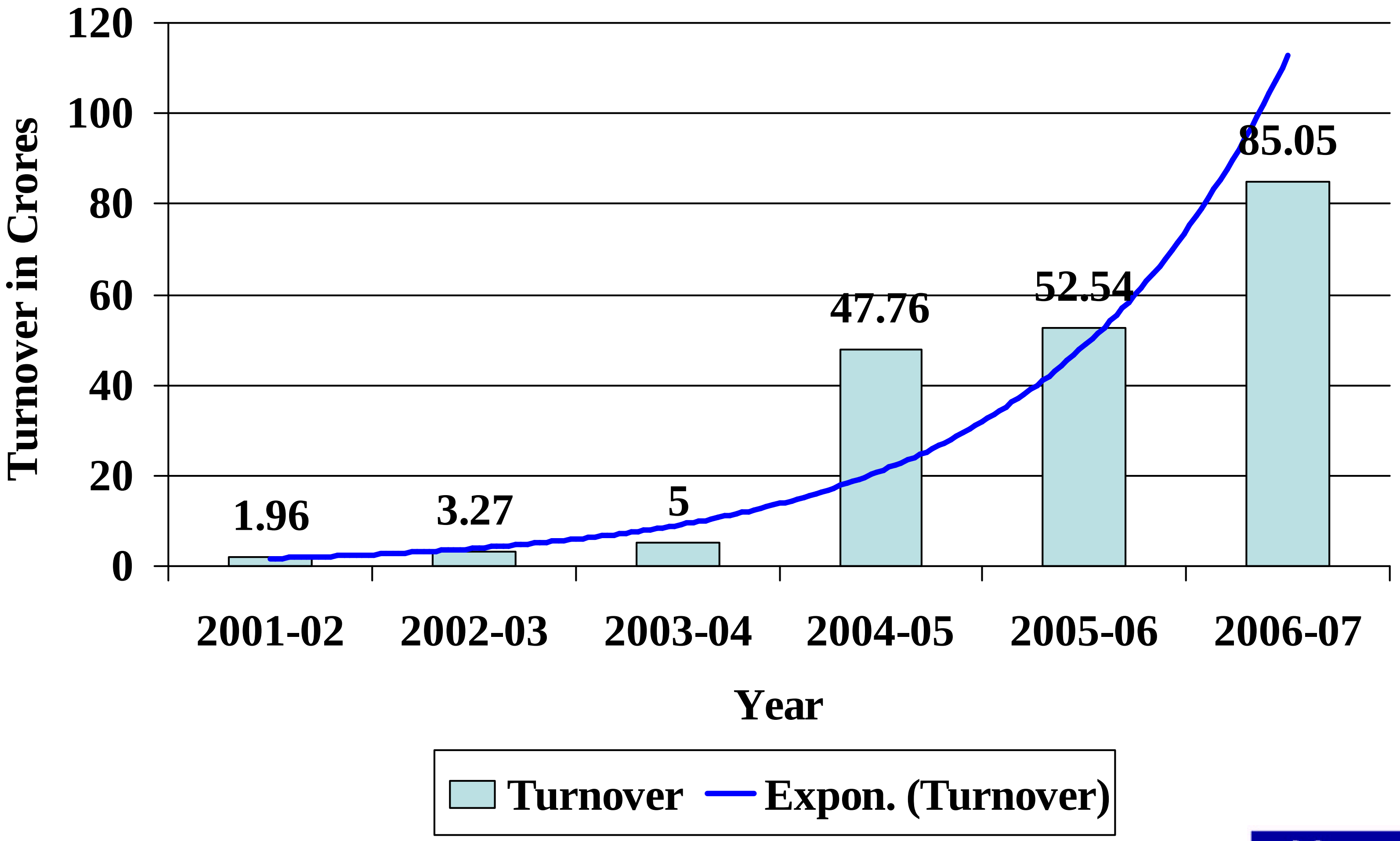
- Incorporated in the year 2000
- Primary focus on Telecom and IT Solutions & Services
- Active Player in India & South East Asia
- Wealth of experience in Turn Key projects
- Technical resource Pool – Juniper, Sun, Cisco, Nortel, Dorado
- Nationwide Presence
  - Headquarter in Delhi
  - Currently executing projects across 40 cities in India
  - Offices in Bangalore & Mumbai

Houston
Technologies Ltd.

Area of Operations

- System Integration
- Operational Support Systems (OSS)
- Business Support Systems (BSS)
- Network Operations & Management
- Software Development
- Consulting Services

OUR GROWTH OVER THE YEARS



Houston
Technologies Ltd.

Major Projects Executed

- **BSNL MPLS Network – (20 cities)**
  - Deployment of the OSS system
  - Operations and Maintenance of the network

- **Railtel MPLS Network – (38 sites)**
  - Turn-key project for deployment of a 38 city MPLS Backbone network including:
    - Network Infrastructure
    - OSS Infrastructure

- **Telekom Malaysia**
  - OSS Integration

- **BSNL Broadband Network**
  - Deployment of OSS
    - Deployment of Subscriber activation System
    - Development of Network Element mediation cartridges
    - Development of Order and Service Inventory System
    - Integration with other OSS/BSS components

Major Projects Executed

- **MTNL Broadband Network – Mumbai & Delhi**
  - Deployment of OSS
    - Deployment of Subscriber activation System
    - Development of Network Element mediation cartridges
    - Integration with other OSS/BSS components

- **BSNL SSTP Network – Phase1 (10 cities), Phase2 (14 cities)**
  - Turnkey supply and deployment of Data Networking components for the SSTP network being set up by BSNL.

- **Indian Air Force Network – (5 cities)**
  - Supply, installation, integration, commissioning and testing of all the proposed equipment at the 5 locations within IAF premises.

- & Many more……..

O & M Projects

- **Railtel – Team (20 people)**
  - Delhi NOC (Helpdesk, L1 & L2 Engineers – 24x7)
  - Secunderabad NOC (L1 Engineers – 24x7)
  - Bombay NOC (L1 Engineers – 24x7)
  - Kolkatta NOC (L1 Engineers – 24x7)

- **BSNL - AMC of the MPLS project – Team (6 people)**
  - Bangalore NOC
  - Thane DR NOC

Wireless Communication

History

In the history of wireless technology, the demonstration of the theory of electromagnetic waves by Heinrich Rudolf Hertz in 1888 was important. The theory of electromagnetic waves were predicted from the research of James Clerk Maxwell and Michael Faraday. Hertz demonstrated that electromagnetic waves could be transmitted and caused to travel through space at straight lines and that they were able to be received by an experimental apparatus.

David E. Hughes, induced electromagnetic waves in a signaling system. Hughes transmitted Morse code by an induction apparatus.

In 1878, Hughes's induction transmission method utilized a "clockwork transmitter" to transmit signals.
In 1885, T. A. Edison uses a vibrator magnet for induction transmission.
In 1888, Edison deploys a system of signaling on the Lehigh Valley Railroad.
In 1891, Edison attains the wireless patent for this method using inductance

What is Wireless Communication?

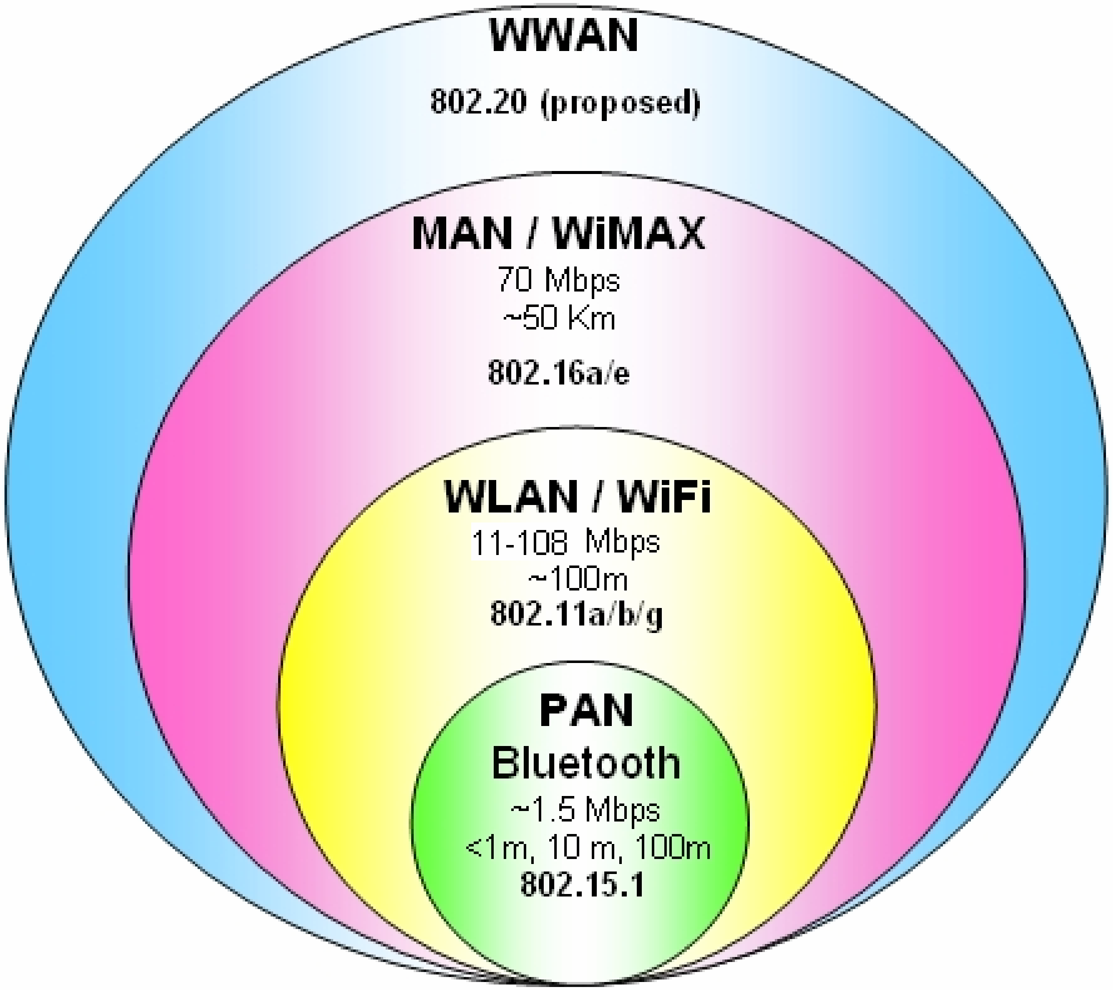
- Any form of communication that does not require the transmitter and receiver to be in physical contact
- Electromagnetic wave propagated through free-space
  - Radar, RF, Microwave, IR, Optical
- Simplex: one-way communication (e.g., radio, TV)
- Half-duplex: two-way communication but not simultaneous (e.g., push-to-talk radios)
- Full-duplex: two-way communication (e.g., cellular phones)

Wired Vs Wireless

- Mobility.
- Elimination of unsightly cables.
- Less installation time.
- Devices can be “software” upgraded to meet new standards
- Guests can connect and move around freely.

- Security.
- Multiple Standards
- Coverage - But the potential for radio interference due to weather, other wireless devices, or obstructions like walls can happen in wireless.

Technologies



Houston
Technologies Ltd.

Bluetooth

- A connection between two or more portable devices without the need for cables or connectors
- The transceiver transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally
- The maximum range is 10 meters.
- Data can be exchanged at a rate of 1 megabit per second (up to 2 Mbps in the second generation of the technology).
- A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference.
- Built-in encryption and verification is provided.

Piconet

subnet of Bluetooth devices, synchronized to the timing and hopping sequence of a master

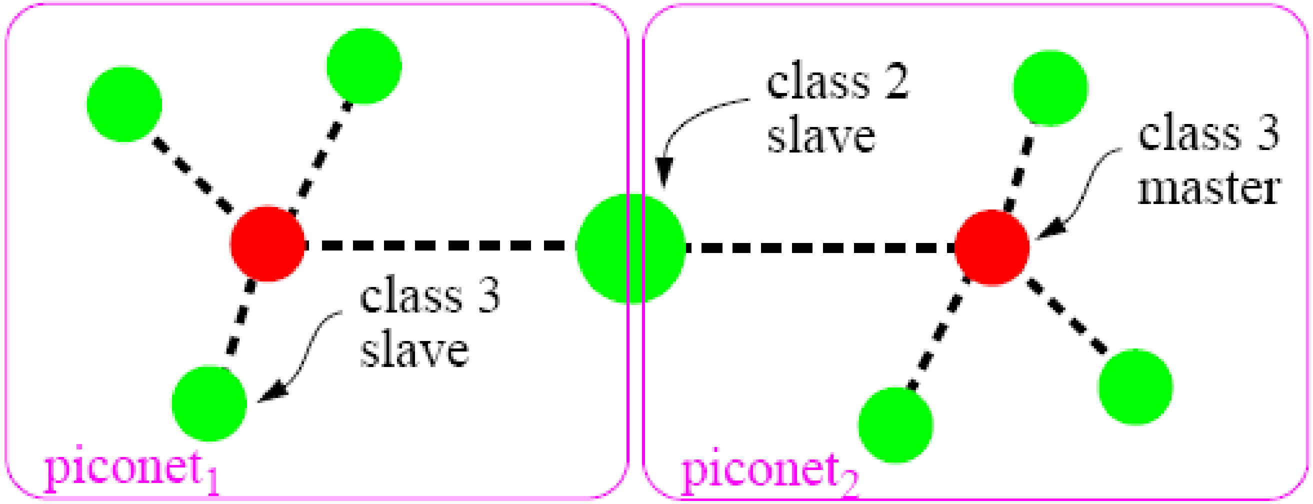
- slaves only communicate with the master
- maximum of 7 slaves in a piconet (as there are only 3 address bits!)

Scatternet

multiple Bluetooth piconets joined together by devices that are in more than one piconet

- Routing of packets between piconets is not defined)

Scatternet



Uses

- Wireless headsets for cell phones.
- If the phone has Internet capability, a Bluetooth piconet can be established between the phone and nearby laptop computer to give the computer, Internet access as well.
- Bluetooth enabled printers can print pictures from a bluetooth enabled cell phone or camera.

Security

- An 8- to 128-bit encryption key can be used to scramble data sent over the link.
- By default, most Bluetooth devices operate in unprotected "non-secure" mode called mode 1.
- mode 2 leaves security up to each authorized application.
- mode 3 secures the entire wireless link.
- For best results, avoid encryption mode 1 (no encryption), choosing either mode 2 (encrypt unicast but not broadcast traffic) or better yet mode 3 (encrypt all traffic).

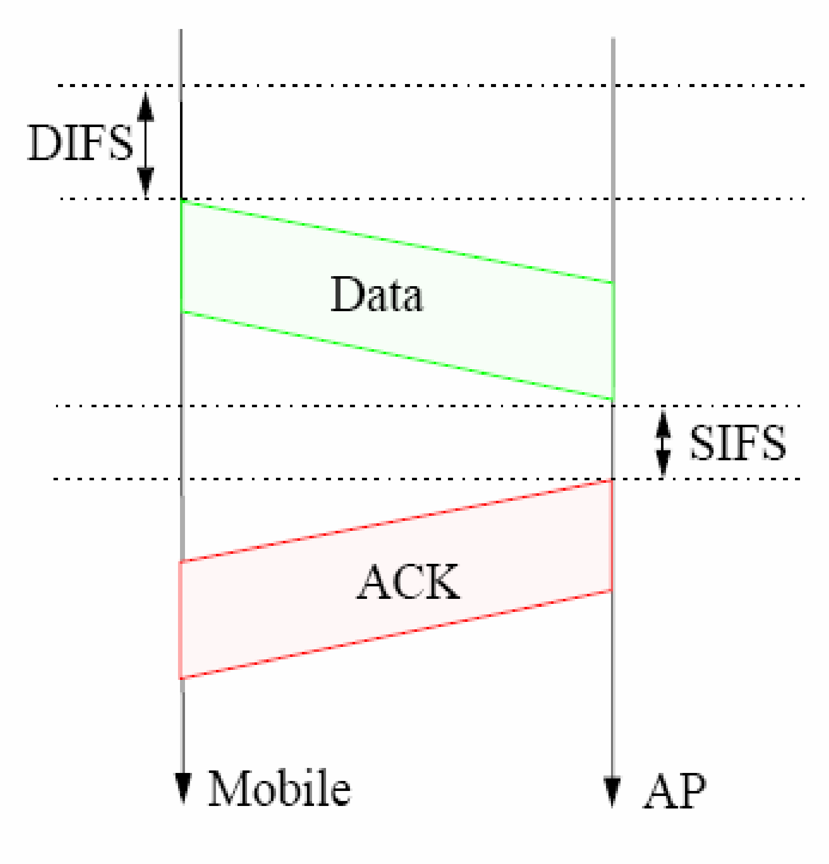
WIRELESS LANs

- WLAN is a flexible data communication system.
- WLANs combine data connectivity with user mobility, and through simplified configuration, enable movable LANs
- An extension to a current wired network or an alternative to it.

Distribution Coordinating Function (DCF)

Distribution Coordinating Function (DCF) is based on carrier sense multiple access with collision avoidance (CSMA/CA).

Receivers send an ACK if they successfully receive a packet, otherwise the transmitter resends.



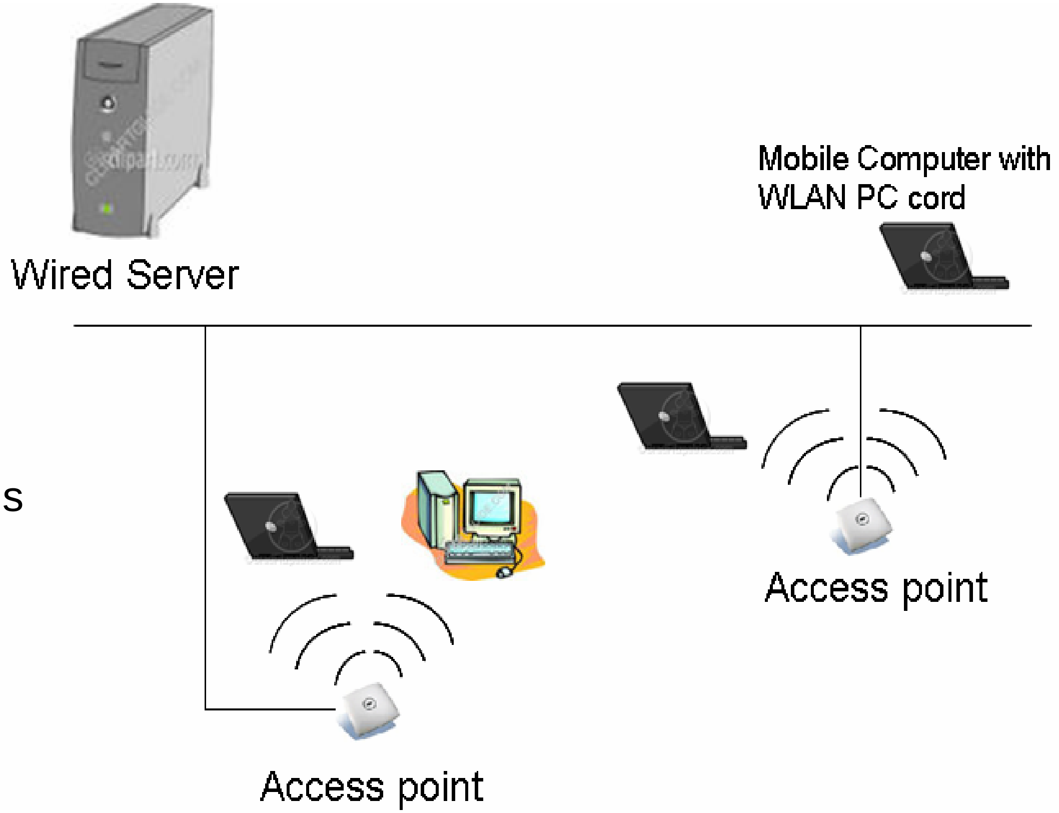
CSMA/CA with ACK in infrastructure network

History

- 1997 the IEEE approved 802.11, which specified the characteristics of devices with a signal rate of 1 and 2 Mb/s.
- The standard specifies the MAC and the physical layers for transmissions in the 2.4 GHz band.
- 1999, the IEEE ratified a new amendment, called IEEE 802.11b, which works at additional signal rates of 5.5 and 11 Mb/s.
- Hereinafter, to the IEEE 802.11 standards as Wi-Fi (Wireless-Fidelity), certifying device interoperability.
- 1999, the IEEE approved the specifications of 802.11a, which uses the 5 Ghz band. The signal rates are 6, 9, 12, 18, 24, 36, 48 and 54 Mb/s.
- In 2003, the IEEE approved 802.11g as a further evolution of the 802.11 standard.
- 802.11g provides the same performance as 802.11a, while working in the 2.4 GHz band. Compatible with 802.11b devices.

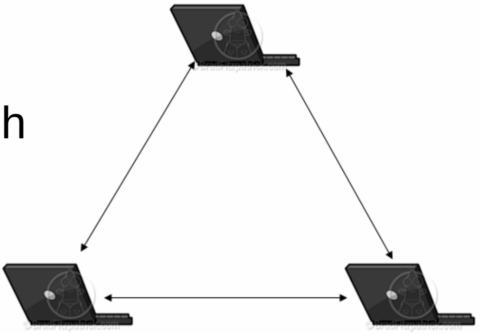
How WLANs Work

- Wireless LANs use electromagnetic airwaves (radio and infrared) to communicate information from one point to another without relying on any physical connection.
- Radio waves are often referred to as radio carriers.
- The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end.
- A transmitter/receiver (transceiver) device, called an *access point,* connects to the wired network from a fixed location using standard Ethernet cable.
- End users access the WLAN through Wireless LAN adapters.
- WLAN adapters provide an interface between the client network operating system (NOS) and the airwaves (via an antenna).
- The nature of the wireless connection is transparent to the NOS.

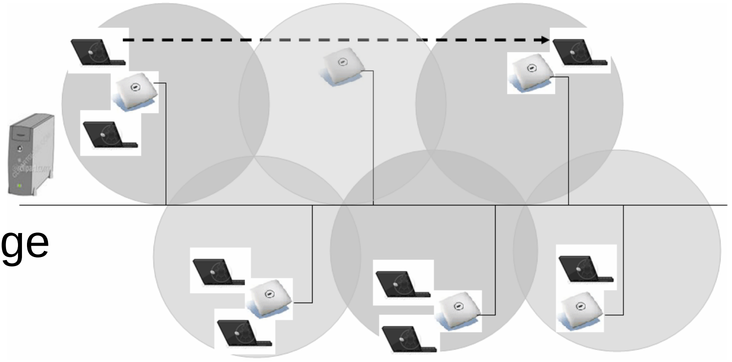


WLAN Configurations

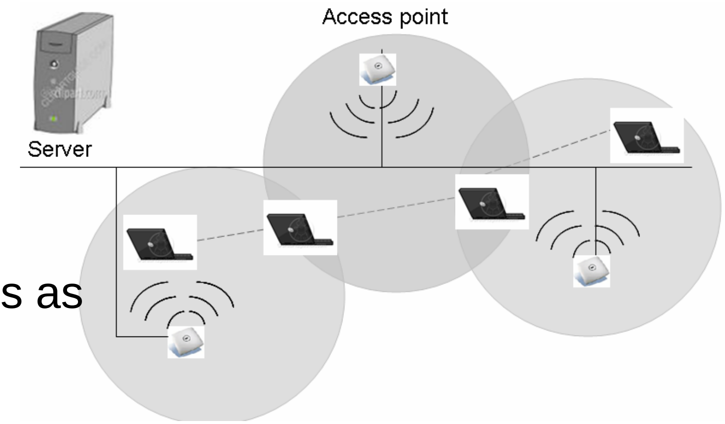
- **Independent WLANs**
  - connects a set of PCs with wireless adapters.
  - Any time two or more wireless adapters are within range of each other, they can set up an independent network.
  - Access points can extend the range of independent WLANs by acting as a repeater.



- **Infrastructure WLANs**
  - Multiple access points link the WLAN to the wired network to efficiently share network resources.
  - Mediate wireless network traffic in the immediate neighborhood.
  - Multiple access points can provide wireless coverage for an entire building or campus.



- **Microcells and Roaming**
  - WLANs use cells, called *microcells,* similar to the cellular telephone system to extend the range of wireless connectivity.
  - Individual microcells overlap to allow continuous communication within wired network.
  - They handle low-power signals and “hand off” users as they roam through a given geographic area.

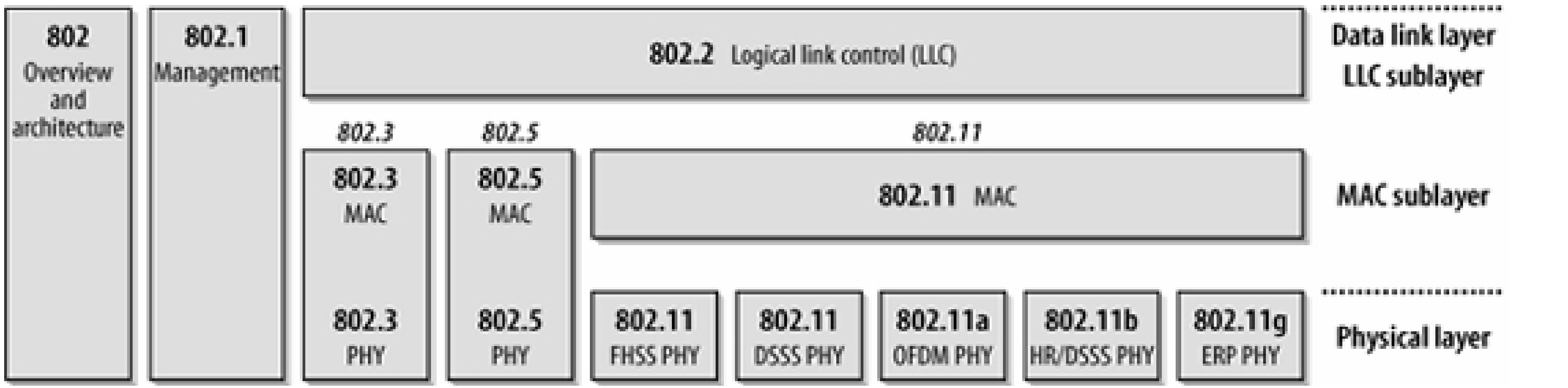


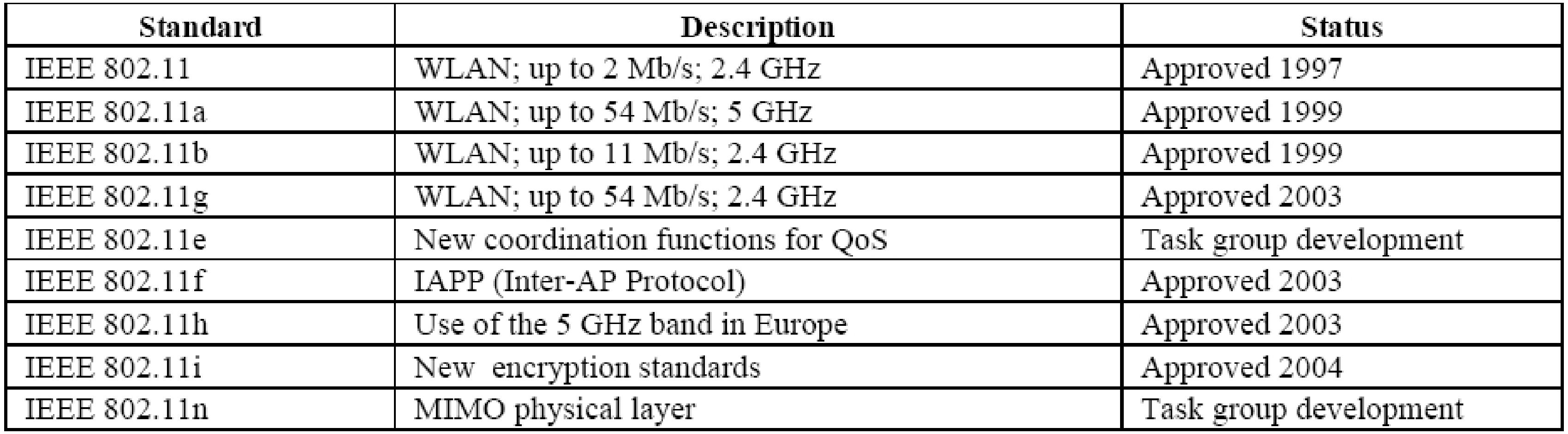
Wireless LAN Technology Options

- Narrowband Technology
  - A narrowband radio system transmits and receives user information on a specific radio frequency.
  - Undesirable crosstalk between communications channels is avoided by carefully coordinating different users on different channel frequencies.
- Spread Spectrum
  - Its a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems.
  - Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security.
- Frequency-Hopping Spread Spectrum
  - It uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.
  - FHSS appears to be short duration impulse noise.
- 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).
  - DSSS appears as low-power wideband noise and is rejected (ignored) by most narrowband receivers.
- Infrared Technology
  - Infrared (IR) systems use very high frequencies, just below visible lighting the electromagnetic spectrum, to carry data.
  - High performance directed IR is impractical for mobile users.
  - Diffuse (or reflective) IR WLAN systems do not require line-of sight, but cells are limited to individual rooms.

Wireless LAN standards – 802.11

802.11 is a member of the IEEE 802 family, including several standards.
The standards define transmission protocols and bandwidth





Standard	Description	Status
IEEE 802.11	WLAN; up to 2 Mb/s; 2.4 GHz	Approved 1997
IEEE 802.11a	WLAN; up to 54 Mb/s; 5 GHz	Approved 1999
IEEE 802.11b	WLAN; up to 11 Mb/s; 2.4 GHz	Approved 1999
IEEE 802.11g	WLAN; up to 54 Mb/s; 2.4 GHz	Approved 2003
IEEE 802.11e	New coordination functions for QoS	Task group development
IEEE 802.11f	IAPP (Inter-AP Protocol)	Approved 2003
IEEE 802.11h	Use of the 5 GHz band in Europe	Approved 2003
IEEE 802.11i	New encryption standards	Approved 2004
IEEE 802.11n	MIMO physical layer	Task group development

b – available several years, 11Mbit/s, 2.4GHz, not standardized 22Mbits in 2.4GHz band of several vendors (sometimes called b+, channel bundling)

g – defined 2003, 108Mbits, 2.4GHz, OFDM (orthogonal frequency division multiplexing)

- most of the hardware sold at the moment confirms to this standard
- backward compatible to “b”, but then more overhead compared to “clean” g standard networks (preamble an initialization sequence must be handled within b standard)

a – 54Mbit/s standard for the 5GHz band, 12 non-overlapping channels, OFDM, restricted output power,

Introduction of transmit power control (TPC) and dynamic frequency selection (DFC),

DFS should reduce the transmission power so it is sufficient for a given connection but does not spread farther than needed,

it checks if the used frequency is free and sufficient,

if not tries to switch over to another frequency with DFC band is reserved for WLAN only, range is more restricted than with 802.11b,

bandwidth is increased up to 108Mbit/s

More standards defining several other aspects of WLANs

c – wireless bridging

d – world mode (combined definitions for different countries)

e – quality of service (QoS on layer 2), packet priorization for real time multimedia and Voice over IP

f – general definition of roaming between access points (of different vendors)

i – authentication and encryption

k – better measurement of WLAN parameters for increase of signal quality, dense networks and location based services (LBS)

m – summarization of extensions to the protocol

extension of bandwidth up to 108-320Mbit/

WLAN Customer Considerations

- Range/Coverage.
- Throughput.
- Integrity and Reliability
- Interoperability with wired Infrastructure.
- Interoperability with wireless Infrastructure.
- Interface and Coexistence.
- Simplicity/Ease of Use.
- Security.
- Cost.
- Scalability.
- Battery life for mobile platforms.
- Safety.

Benefits of WLANs

- *Improves productivity and service.*
- *Installation Flexibility.*
- *Reduced Cost-of-Ownership.*
- *Scalability.*
- *Mobility improves productivity and service.*
- *Installation Speed and Simplicity*

Wireless Networking Challenges

- Disconnection
- Low Bandwidth
- Variable Bandwidths
- Security risks
- Mobility
- Power consumption

Applications for Wireless LANs

- Hospitals
- Consulting or accounting audit teams.
- In dynamic environments minimize the overhead of moves, adds, and changes with wireless LANs.
- Used on Training sites at corporations and students at universities .
- Easy setup in older buildings
- Retail store IS managers use wireless networks to simplify frequent network reconfiguration.
- Warehouse workers use wireless LANs to exchange information with central databases and increase their productivity.
- To backup for mission-critical applications running on wired networks.
- Real-time customer information input and retrieval.
- Real-time information at their fingertips.

Security

WEP (Wired Equivalent Privacy): It is a weak, standalone encryption method. Simply encrypts the data traffic between the wireless access point and the client computer. It doesn't actually secure either end of the transmission. Also, the encryption level is 40 bits, which now is considered very weak.

WPA (Wi-Fi Protected Access): WPA implements higher security and addresses the flaws in WEP. When used in PSK (pre-shared key) mode, WPA-PSK is considered safe enough for most home and small business use, and when combined with technologies like RADIUS and VPN, is considered secure enough for all but the most sensitive enterprise applications.

802.1x: WPA consists of a pair of smaller standards that address different aspects of security: TKIP (Temporal Key Integrity Protocol encryption), which is what encrypts the wireless signal, and 802.1x, which handles the authentication of users to the network. 802.1x makes you authenticate to the wireless network itself, not an individual access point, and not to some other level like VPN. This is more secure, as unauthorized traffic can be denied right at the wireless access point.

802.11i: It combines with the highest level of encryption for a wireless connection (called Advanced Encryption Standard [AES]). It supports key sizes of 128 bits, 192 bits and 256 bits.

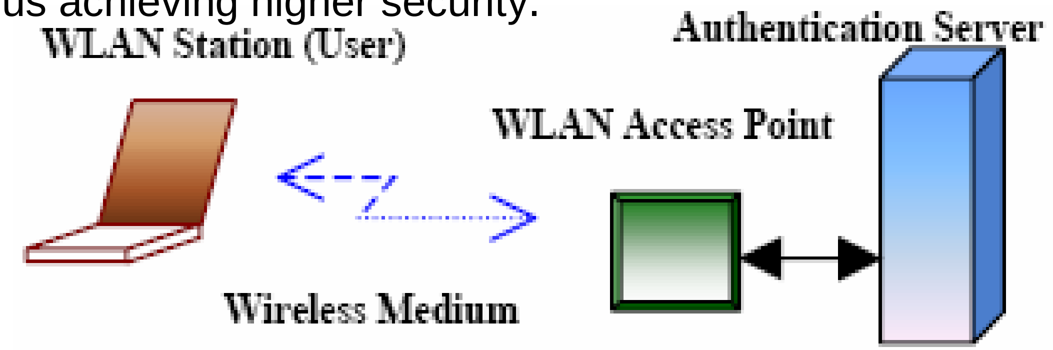
IEEE 802.1x (Port based Authentication)

The WLAN security can be broken down into three components--authentication mechanism, authentication algorithm and data frame encryption.

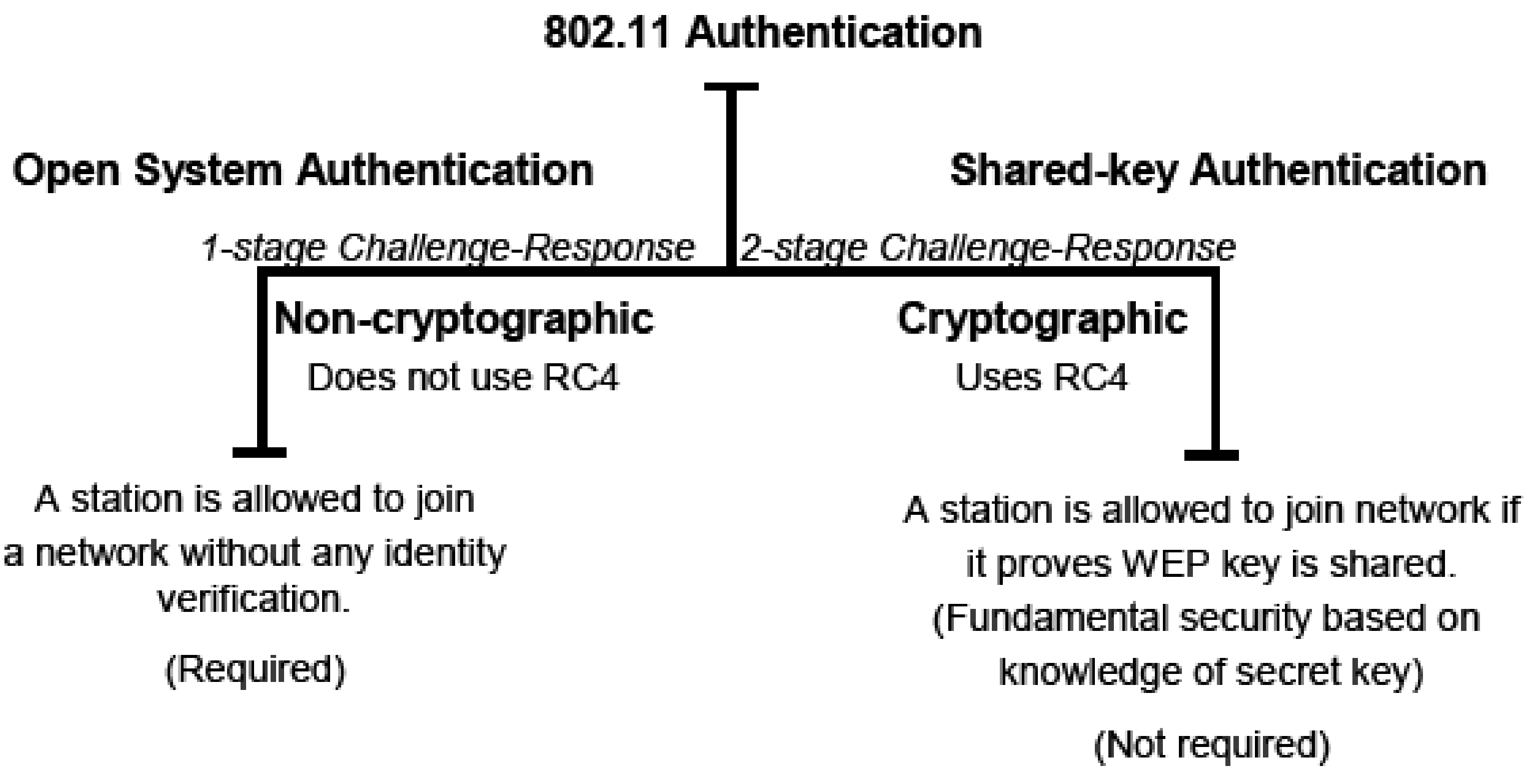
The IEEE 802.1x frames are treated as authentication message carriers. When the client starts establishing wireless connection, it sends the authentication message inside the IEEE 802.1x frame to the AP (Access Point). The AP then forwards that frame to the centrally located authentication server (like RADIUS server).

The Authentication server is configured with the required information to authenticate the clients. It accepts or rejects the packets and thus replies to the AP whether the client is an authorized user or not. The AP accepts messages from the client only after the authentication server authenticates the client.

IEEE 802.1x also has a built-in key management protocol that dynamically distributes the WEP keys. This feature can be used by the AP to periodically pass on a new key to the client. The new key is used both by the client and the AP for the WEP encryption/decryption of the subsequent data packets exchanged, thus achieving higher security.



Authentication



802.11 Authentication

Open System Authentication

1-stage Challenge-Response

Non-cryptographic

Does not use RC4

A station is allowed to join a network without any identity verification.

(Required)

Shared-key Authentication

2-stage Challenge-Response

Cryptographic

Uses RC4

A station is allowed to join network if it proves WEP key is shared. (Fundamental security based on knowledge of secret key)

(Not required)

Bluetooth	Wi-Fi
Lower cost	Higher cost
Uses less power	Uses more power
Data Rate=1Mbps	Data Rate=11 Mbps
Typical distance=100 feet	Typical distance=300 feet
Use to replace cable	Use to access Ethernet without cables or wires to become WLAN
PAN (Personal Area Network)	(Wireless Local Area Network)
Ad-hoc network (links notebooks with cell phone or PDA	Excellent for corporate infrastructure, small business/home business LAN-in-a-box)
Localized voice connectivity	Extension or replacement of a wired LAN infrastructure

Wireless Controllers

- A device that can manage APs directly or indirectly connected to it on the network.
- Gives system wide wireless LAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility

The following types of management are widely used:

Command Line Interface (CLI).

Each WLAN product is managed by locally configuring them from their console.

Web-Based Management.

The configuration and monitoring of WLAN is done by using a standard web browser.

SNMP Management

The WLAN products are managed from the SNMP manager.

Telnet based Management

The administrator can telnet from remote machine and do the necessary configuration.

Mobility

Allowing the user to use his computer anywhere to access network resources without the traditional network cable.

Roaming within the subnet	**Roaming across the subnet**
Easier to Implement	Difficult to implement
IAPP (Inter Access Point Protocol) is a standard WLAN protocol to roam within the subnet.	Roaming across the subnet is addressed by the Mobile IP protocol.

IAPP for Roaming within the same subnet

IAPP defines the procedures for AP to AP communication. On a WLAN when a user moves from one BSS to another his association with the older AP gets dissociated and gets associated with the AP of the newer BSS. As the user returns back to the older BSS, his identity gets re-associated. The user's identity and BSS, to which he is currently associated, are conveyed to other APs by the IAPP protocol.
The IEEE 802.11b allows freedom to WLAN vendors for implementing their own roaming protocol, such as IAPP. This may give rise to interoperability issue between the products of various vendors. So a new standard, IEEE 802.11f, that addresses the interoperability issues and facilitates a common framework is currently under development.

Mobile IP for Roaming across subnets

Mobile IP is a standard that is described in RFC 2002. This standard specifies a protocol that allows transparent routing of IP datagrams to mobile nodes, which roam across various subnets (anywhere in the internet). This standard needs to be implemented in both the Client (Station) and as well as in the AP. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. When situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

WiMax

- Worldwide Interoperability for Microwave Access
- Providing wireless data over long distances in a variety of ways
- Based on the IEEE 802.16 standard, which is also called WirelessMAN.
- “A standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL.“
- Can route data to Wi-Fi
- Wi-Fi devices can take advantage of WiMAX connection.
- Connection up to 70 Mbps over the area of 30 miles.
- There is no need for line of sight connection between subscriber terminals and the base station in WiMAX it can support hundreds of subscribers from a single base station.

Applications

- Connecting Wi-Fi hotspots with each other and to other parts of the Internet.

- Providing a wireless alternative to cable and DSL for last mile broadband access.

- Providing high-speed data and telecommunications services.

- Providing a diverse source of Internet connectivity as part of a business continuity plan.

- That is, if a business has a fixed and a wireless Internet connection, especially from unrelated providers, they are unlikely to be affected by the same service outage.

- Providing nomadic connectivity.

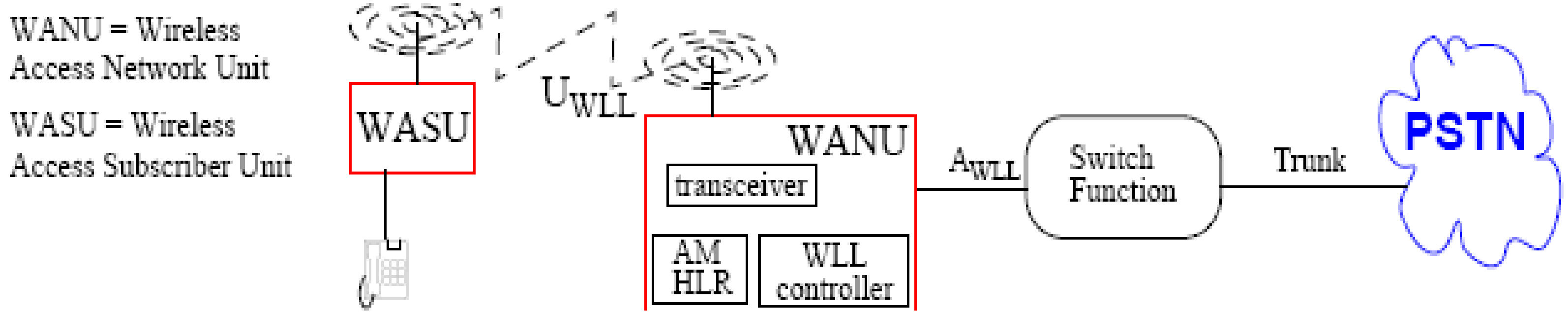
Wireless Local Loop (WLL)

Providing wireless connections to stationary or near stationary stations within a small service area.
Generally targeted at the “last mile” or from a point in the neighborhood to the user.

Advantages of Wireless local loop:

- ease of installation
- reducing digging, reduce poles, ducts/conduits, …
- quick installation of new links (i.e., rapid provisioning)
- largely distance insensitive pricing - at least up to some limit
- concentration of resources (especially at the multiplexer to the high bandwidth backbone)

IS-54 architectural reference model for WLL:



WANU = Wireless Access Network Unit

WASU = Wireless Access Subscriber Unit

WiMAX or Wi-Fi

•WiMAX is a long-range system, covering many kilometers that typically uses licensed spectrum to deliver a point-to-point connection to the Internet from an ISP to an end user.
Wi-Fi is a shorter range system, typically hundreds of meters, that uses unlicensed spectrum to provide access to a network, typically covering only the network operator's own property.

•WiMAX provides services analogous to a cellphone,
Wi-Fi is more analogous to a cordless phone.

•WiMAX uses a mechanism based on setting up connections between the Base Station and the user device. Each connection is based on specific scheduling algorithms, which means that QoS parameters can be guaranteed for each flow.
Wi-Fi has introduced a QoS mechanism similar to fixed Ethernet, where packets can receive different priorities based on their tags. This means that QoS is relative between packets/flows, as opposed to guaranteed.

•WiMAX is highly scalable from remote stations to multi-sector 'maxi' scale base that handle complex tasks of management and mobile handoff functions and include MIMO-AAS smart antenna subsystems.

Wireless WAN

- Enables users to establish wireless connections over remote private or public networks using radio, satellite and mobile phone technologies.

- Uses cellular network technologies such as WIMAX, GPRS, GSM, UMTS, CDMA2000,CDPD, Mobitex, HSDPA or 3G to transfer data.

- It can use also LMDS and Wi-Fi to connect to the Internet.

- These cellular technologies are offered regionally, nationwide, or even globally and are provided by a wireless service provider for a monthly usage fee.

- These connections can be maintained over large geographical areas, such as cities or countries, through the use of satellite systems or multiple antenna sites maintained by wireless service providers.

- Schools or a businesses in rural areas benefit from Wireless WANs because it is more cost effective than laying long cable or fibre links.

- The same can be said for institutions in built up urban areas. Installing cable into an existing location could be very disruptive, so a wireless alternative is more cohesive.

Examples of Wireless WANs

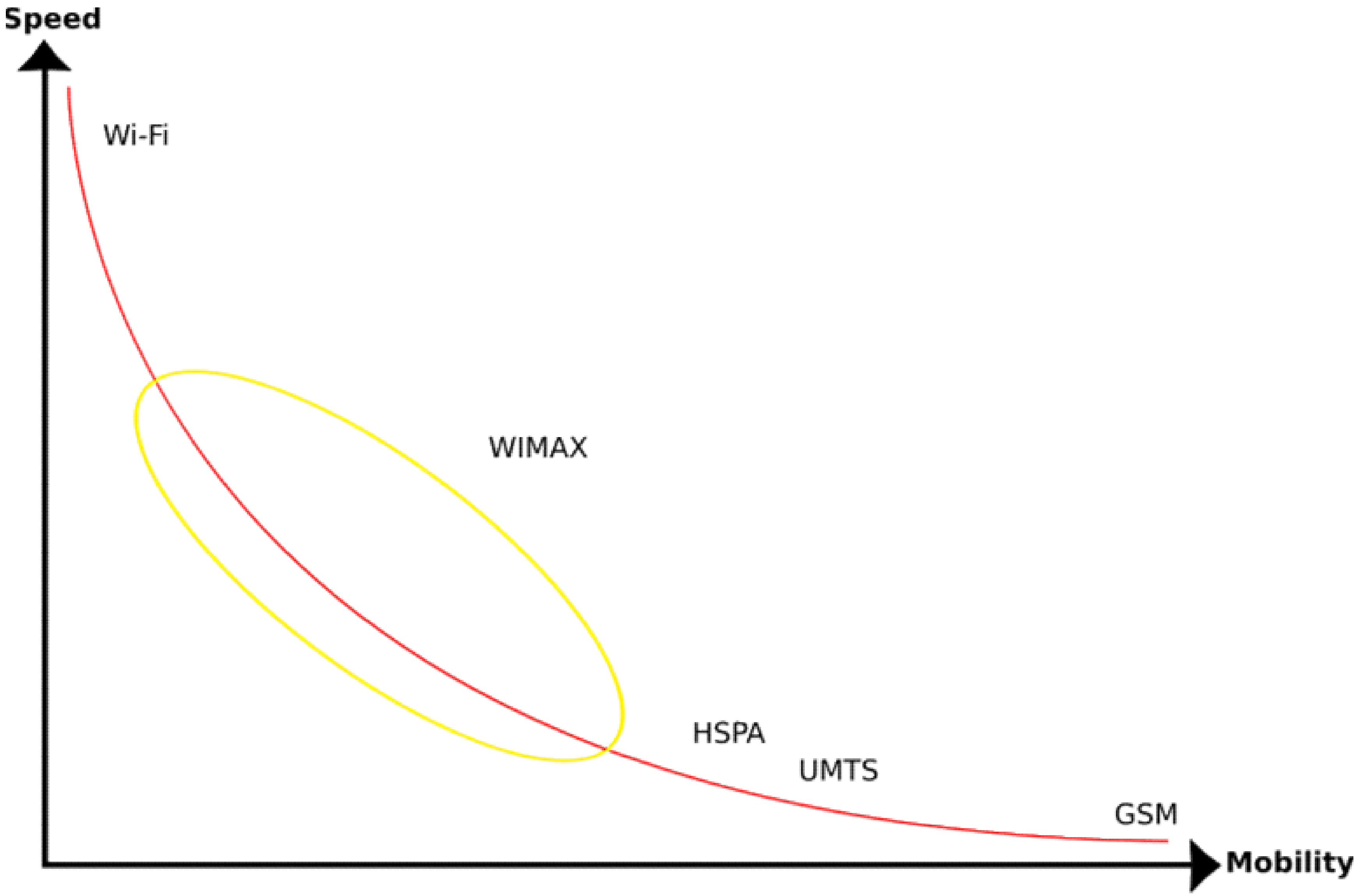
- Digital Cellular Phone and Data Services,

- Satellite Modems or a computer hooked up with a wireless WAN card and used in a city or geographical area that has WWAN deployed.

- There are cities that offer wireless internet services to the anyone who lives within it's reach.

- Some universities offer WWAN services to students who can hook up to the school network from outside of the building or across town.

Competing Technologies



Houston
Technologies Ltd.

THANK YOU

Houston Technologies Limited
Splendor House
F-38/2, Okhla Industrial Area, Phase II,
New Delhi – 110 020, India
Phone: +91-11-26383002/07
Fax: +91-11-26383225
email: **contact@houstontechnologies.com**

Visit our Website: www.houstontechnologies.com
to download this presentation

Houston
Technologies Ltd.