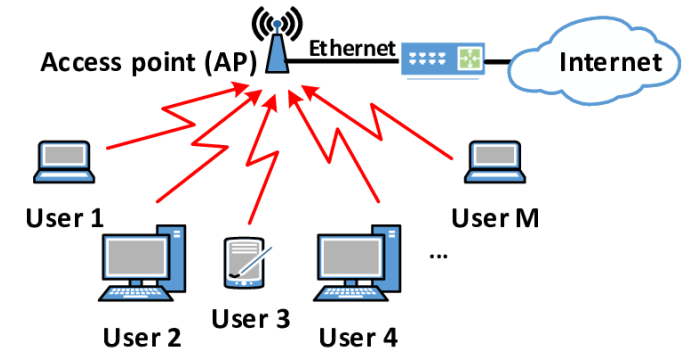


WLAN:IEEE 802.11

Wireless Local Area Network

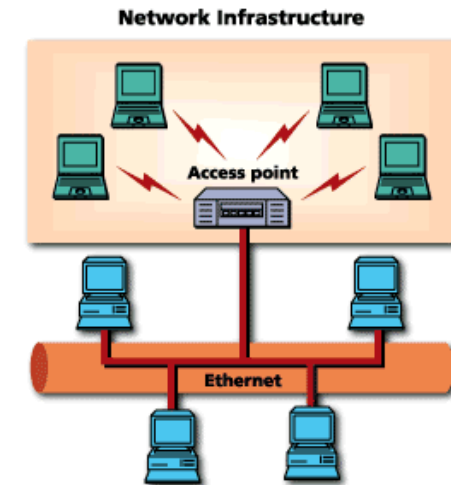
The wireless LAN connects to a wired LAN

- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



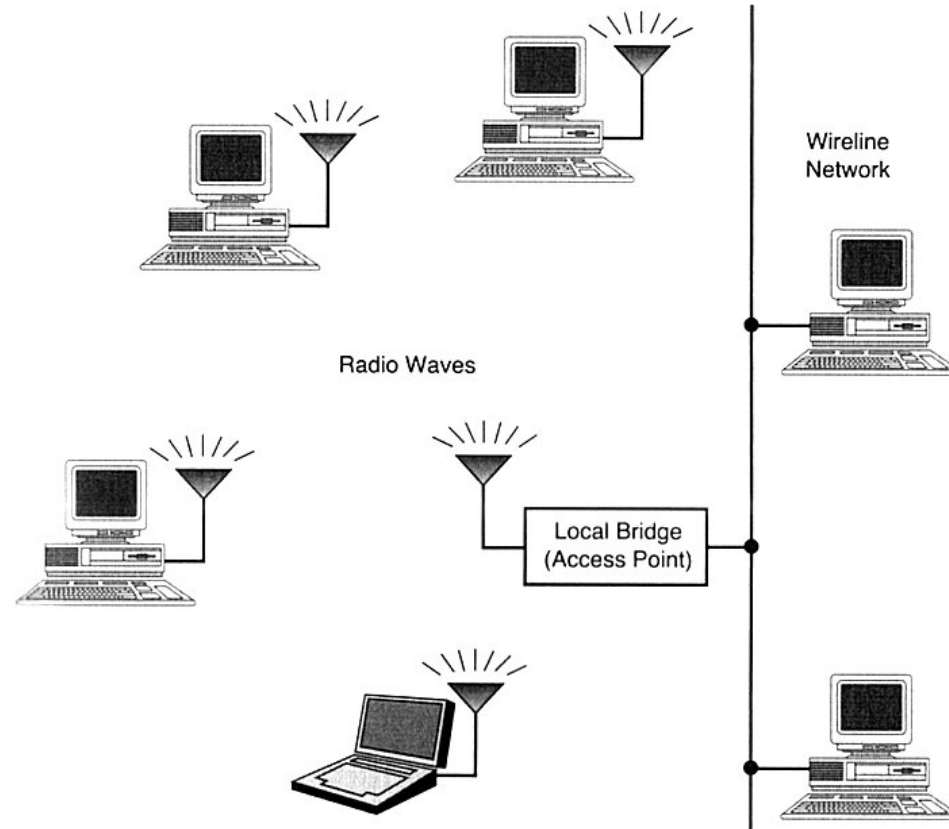
Integration With Existing Networks

- Wireless Access Points (APs) - a small device that bridges wireless traffic to your network.
- Most access points bridge wireless LANs into Ethernet networks, but Token-Ring options are available as well.

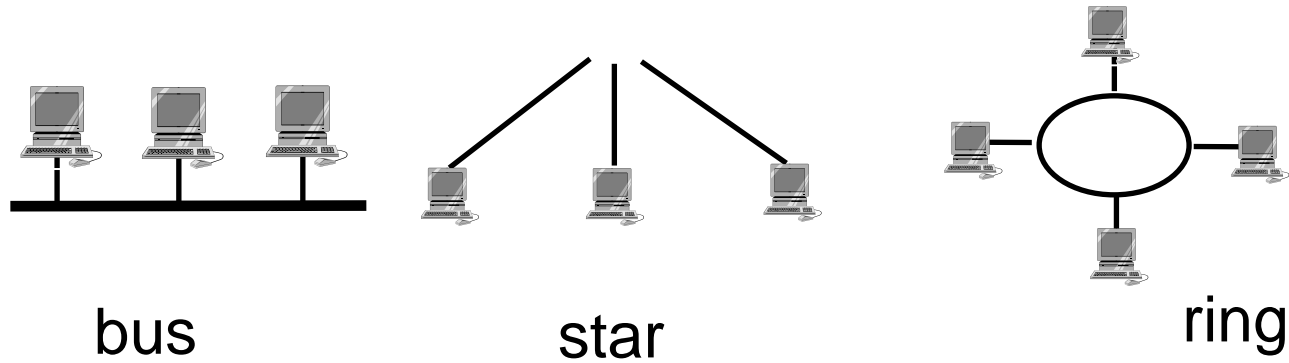
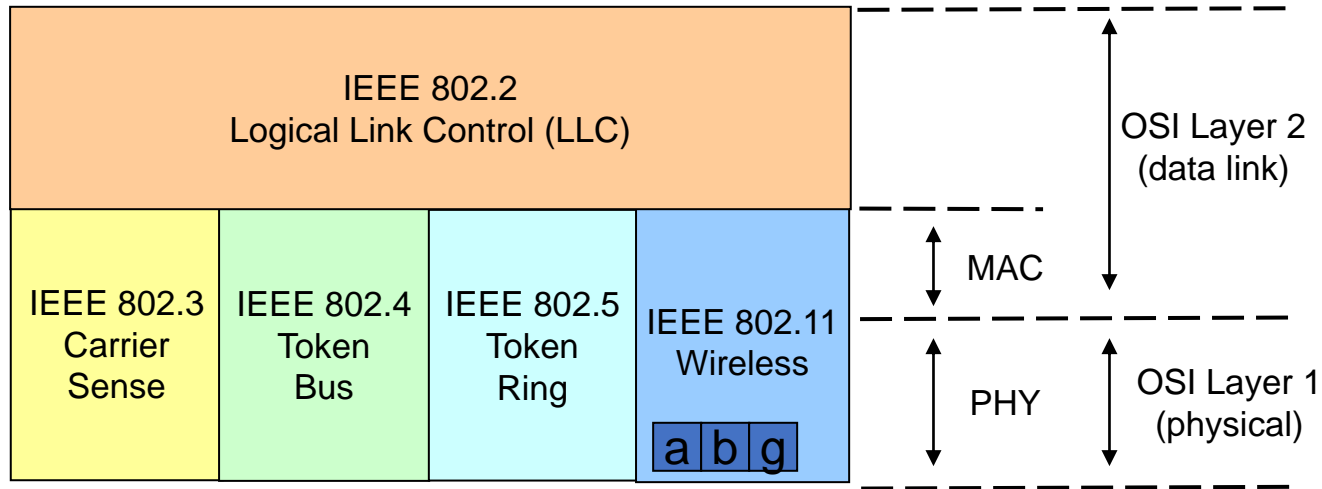


802.11 WLANs - Outline

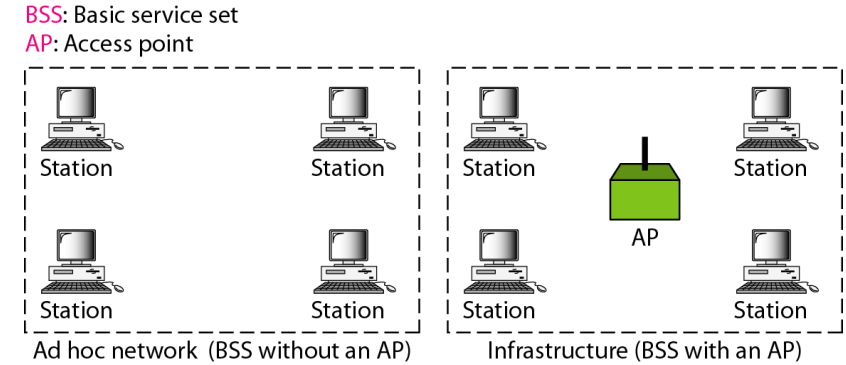
- 801.11 bands and layers
- Link layer
- Media access layer
 - frames and headers
 - CSMA/CD
- Physical layer
 - frames
 - modulation
 - Frequency hopping
 - Direct sequence
 - Infrared
- Security
- Implementation



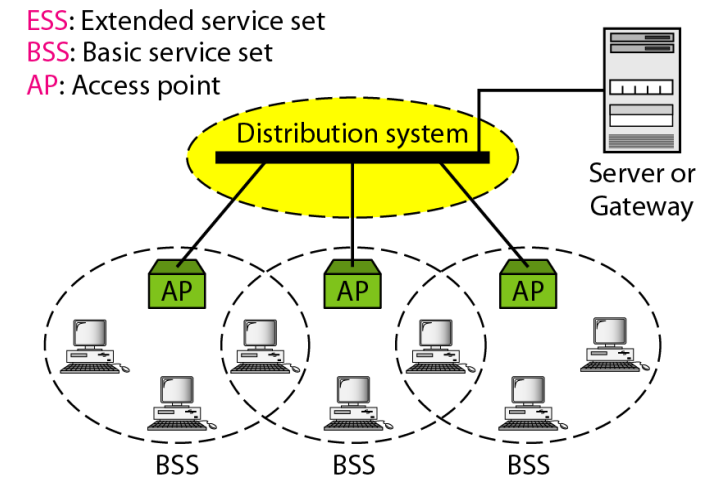
The IEEE 802.11 and supporting LAN Standards



Basic service sets (BSSs)

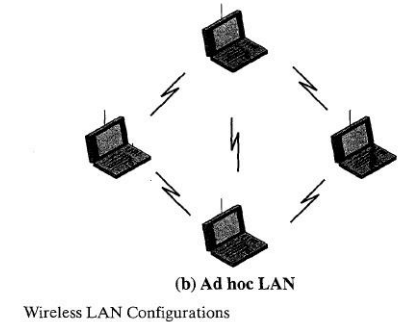
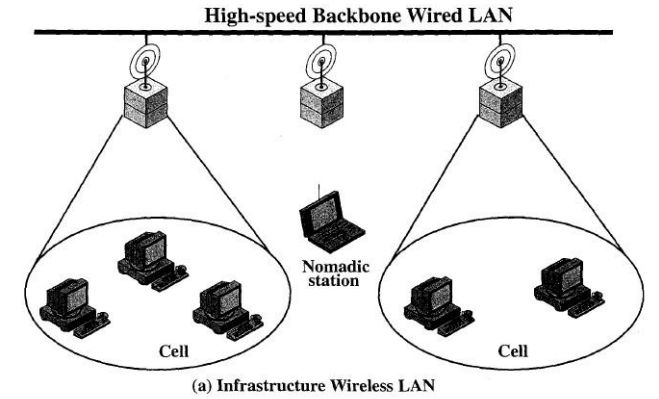


Extended service sets (ESSs)

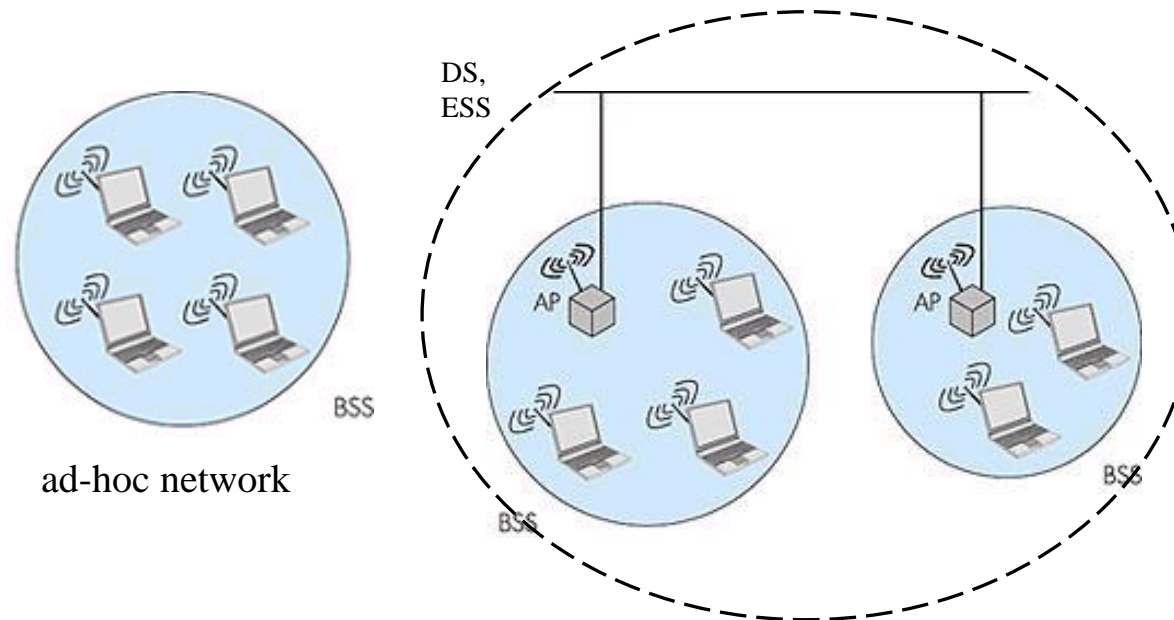


IEEE 802.11 Architecture

- IEEE 802.11 defines the physical (PHY), logical link (LLC) and media access control (MAC) layers for a wireless local area network
- 802.11 networks can work as
 - basic service set (BSS)
 - extended service set (ESS)
- BSS can also be used in ad-hoc networking



LLC: Logical Link Control Layer
 MAC: Medium Access Control Layer
 PHY: Physical Layer
 FHSS: Frequency hopping SS
 DSSS: Direct sequence SS
 SS: Spread spectrum
 IR: Infrared light
 BSS: Basic Service Set
 ESS: Extended Service Set
 AP: Access Point
 DS: Distribution System



802.11 Logical architecture

- LLC provides addressing and data link control
- MAC provides
 - access to wireless medium
 - CSMA/CA
 - Priority based access (802.12)
 - joining the network
 - authentication & privacy
 - Services
 - Station service: Authentication, privacy, MSDU* delivery
 - Distributed system: Association** and participates to data distribution
- Three physical layers (PHY)
 - FHSS: Frequency Hopping Spread Spectrum (SS)
 - DSSS: Direct Sequence SS
 - IR: Infrared transmission

LLC: Logical Link Control Layer
MAC: Medium Access Control Layer
PHY: Physical Layer
FH: Frequency hopping
DS: Direct sequence
IR: Infrared light

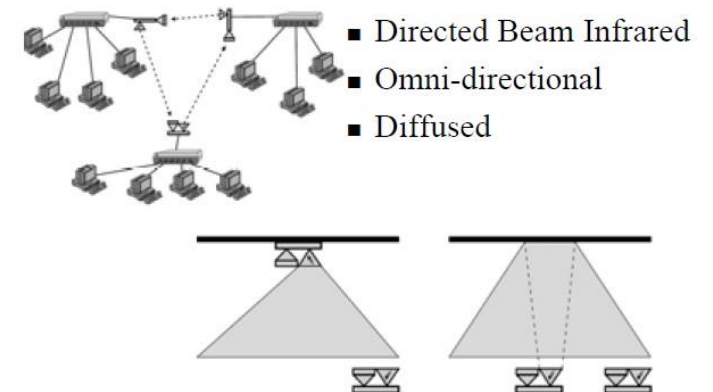
*MSDU: MAC service data unit

** with an access point in ESS or BSS

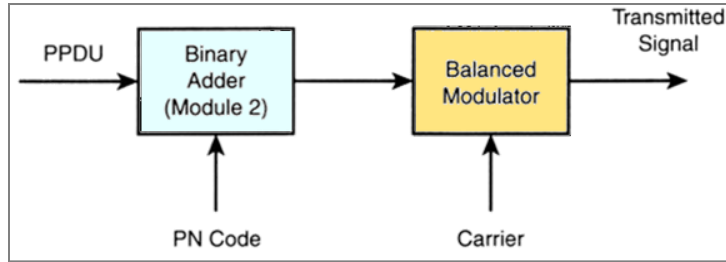
Wireless LAN Categories:

- Infrared (IR) LANs (P2P, Omni Directional, diffused)
- Spread spectrum LANs
- Narrow Band MW

IR Data Transmission Techniques

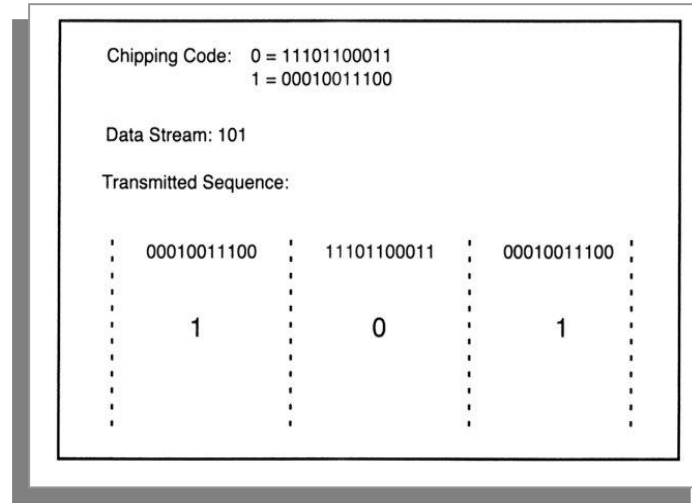


802.11 DSSS



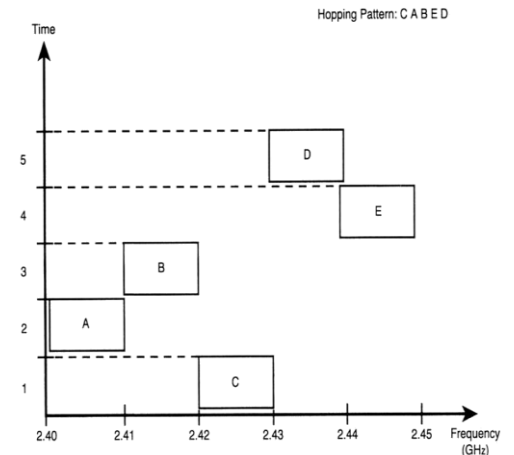
DS-transmitter

- Supports 1 and 2 Mbps data transport, uses BPSK and QPSK modulation
- Uses 11 chips Barker code for spreading - 10.4 dB processing gain
- Defines 14 overlapping channels, each having 22 MHz channel bandwidth, from 2.401 to 2.483 GHz
- Power limits 1000mW in US, 100mW in EU, 200mW in Japan
- Immune to narrow-band interference, cheaper hardware
PPDU: baseband data frame



802.11 FHSS

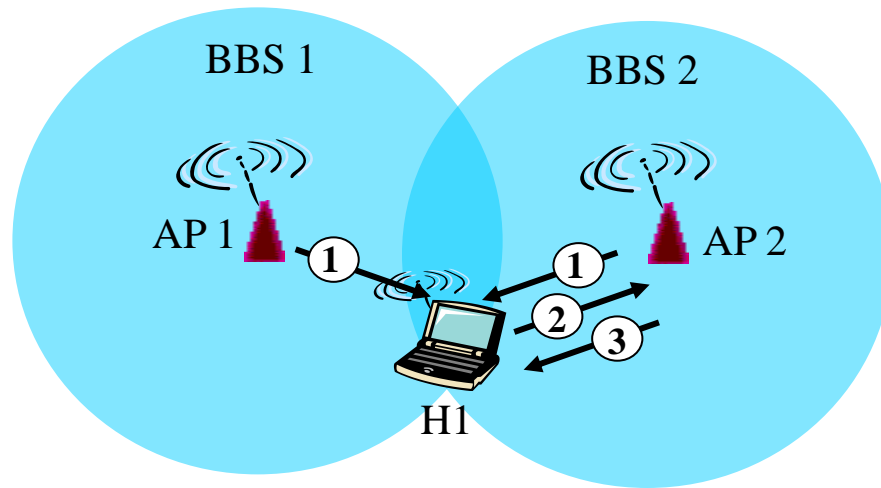
- Supports 1 and 2 Mbps data transport and applies two level - GFSK modulation* (Gaussian Frequency Shift Keying)
- 79 channels from 2.402 to 2.480 GHz (in U.S. and most of EU countries) with 1 MHz channel space
- 78 hopping sequences with minimum 6 MHz hopping space, each sequence uses every 79 frequency elements once
- Minimum hopping rate 2.5 hops/second
- Tolerance to multi-path, narrow band interference, security
- Low speed, small range due to FCC TX power regulation (10mW)



802.11: Channels, association

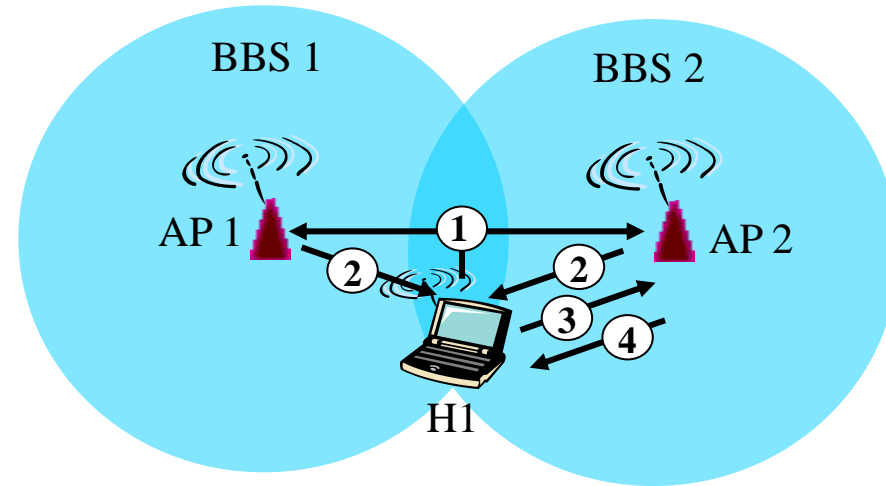
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
 - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
 - selects AP to associate with
 - may perform authentication
 - will typically run DHCP to get IP address in AP's subnet

802.11: Passive/Active scanning



Passive Scanning:

- (1) beacon frames sent from APs
- (2) association Request frame sent: H1 to selected AP
- (3) association Response frame sent: H1 to selected AP

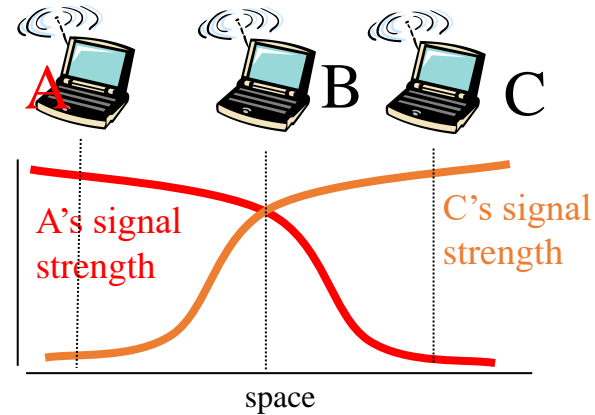
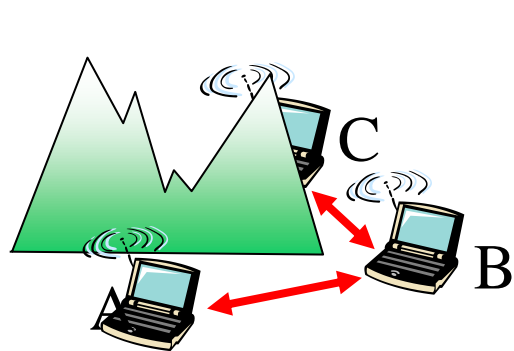


Active Scanning:

- (1) Probe Request frame broadcast from H1
- (2) Probes response frame sent from APs
- (3) Association Request frame sent: H1 to selected AP
- (4) Association Response frame sent: H1 to selected AP

IEEE 802.11: multiple access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
 - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
 - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
 - can't sense all collisions in any case: hidden terminal, fading
 - goal: *avoid collisions*: CSMA/C(ollision)A(voidance)



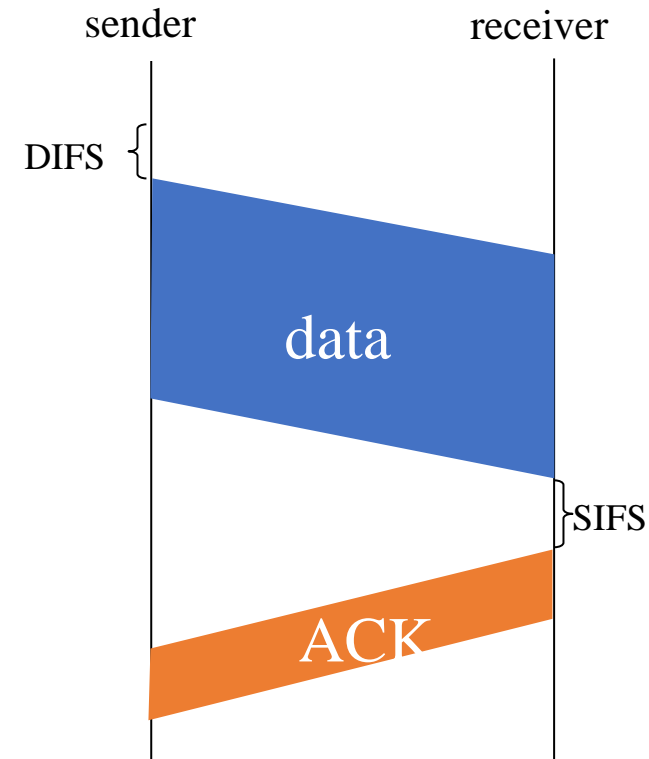
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

- 1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)
- 2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval,
repeat 2

802.11 receiver

- if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)



- DIFS: Distributed condition function (DCF) Interframe Space
- SIFS: Short interframe space

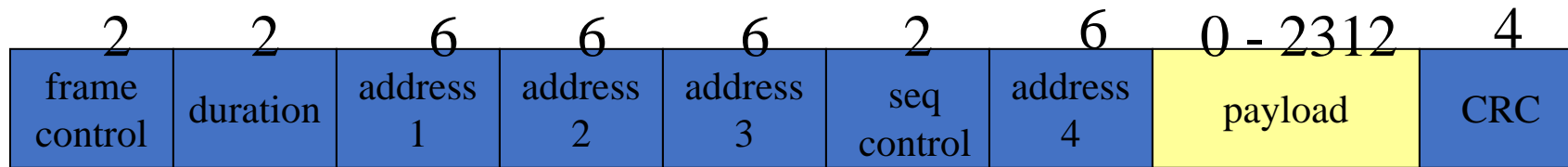
Avoiding collisions (more)

idea: allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
 - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
 - sender transmits data frame
 - other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

802.11 frame: addressing



Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

WLAN benefits

- Mobility
 - increases working efficiency and productivity
 - extends the On-line period
- Installation on difficult-to-wire areas
 - inside buildings
 - road crossings
- Increased reliability
 - Note: Pay attention to security!
- Reduced installation time
 - cabling time and convenient to users and difficult-to-wire cases
- Broadband
 - 11 Mbps for 802.11b
 - 54 Mbps for 802.11a/g (GSM:9.6Kbps, HCSCD:~40Kbps, GPRS:~160Kbps, WCDMA:up to 2Mbps)
- Long-term cost savings
 - O & M cheaper than for wired nets
 - Comes from easy maintenance, cabling cost, working efficiency and accuracy
 - Network can be established in a new location just by moving the PCs!

WLAN technology problems

- Data Speed
 - IEEE 802.11b support up to 11 MBps, sometimes this is not enough - far lower than 100 Mbps fast Ethernet
- Interference
 - Works in ISM band, share same frequency with microwave oven, Bluetooth, and others
- Security
 - Current WEP algorithm is weak - usually not ON!
- Roaming
 - No industry standard is available and propriety solution are not interoperable - especially with GSM
- Inter-operability
 - Only few basic functionality are interoperable, other vendor's features can't be used in a mixed network

Easy Wifi Radar



Produktionsfirma
Für Marketing, Web, Design
www.pfaff.de

Wi-Fi





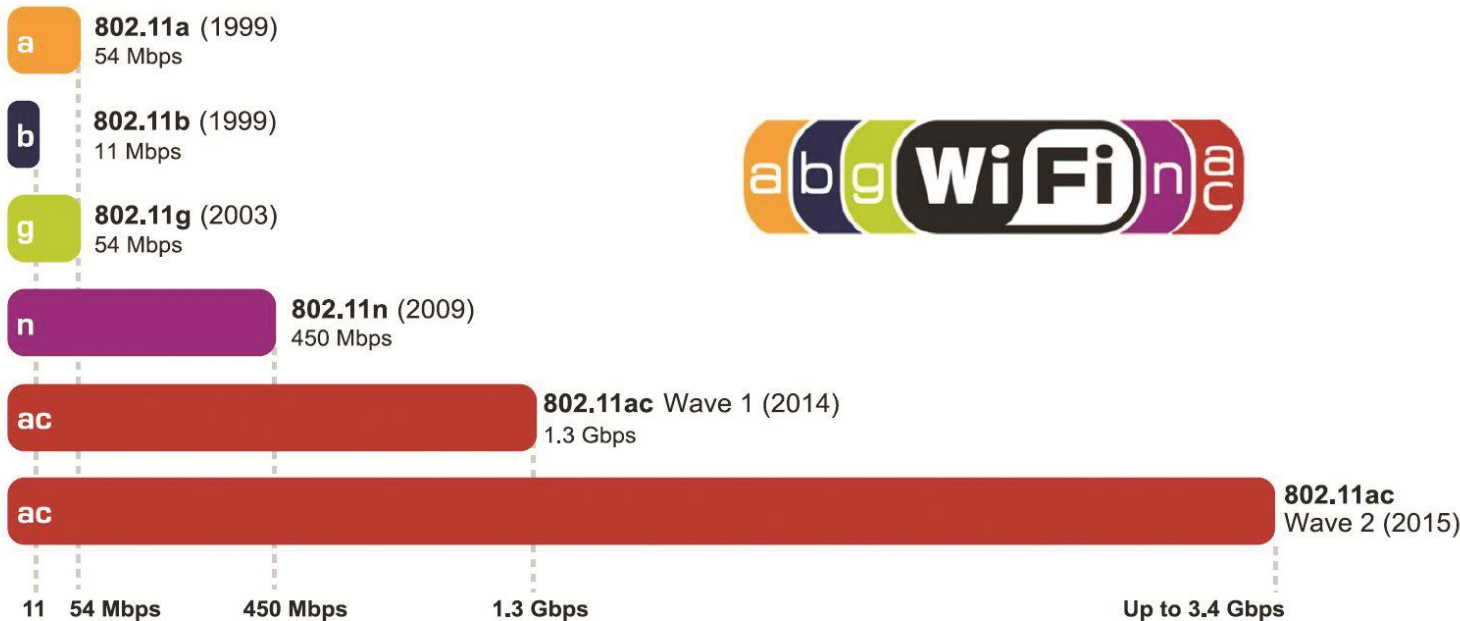
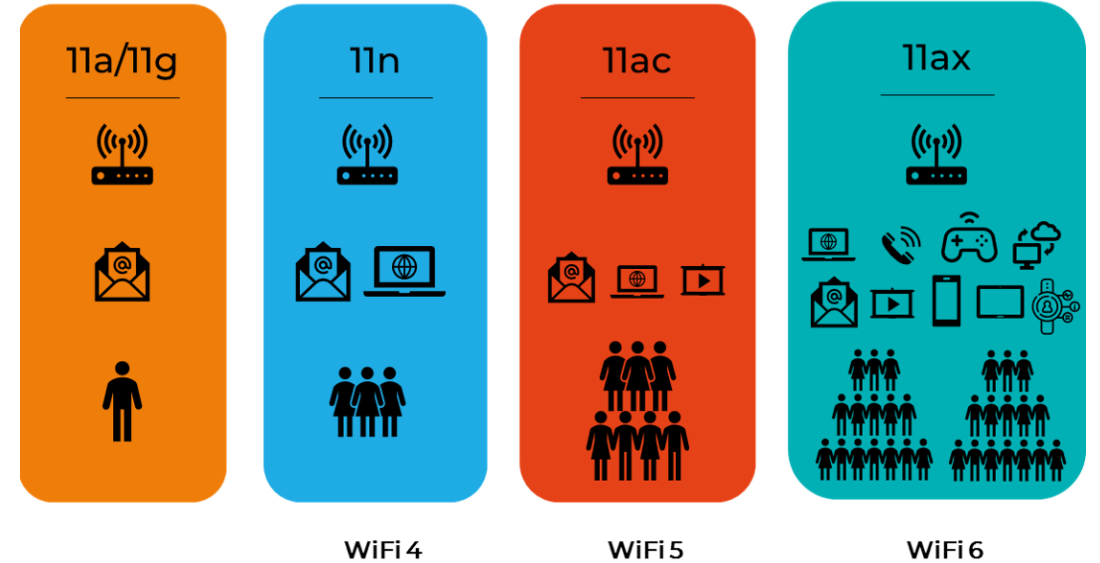
INTRODUCTION

- Wireless Technology is an alternative to Wired Technology, which is commonly used, for connecting devices in wireless mode.
- Wi-Fi (Wireless Fidelity) is a generic term that refers to the IEEE 802.11 communications standard for Wireless Local Area Networks (WLANs).
- Wi-Fi Network connect computers to each other, to the internet and to the wired network.

THE Wi-Fi TECHNOLOGY

Wi-Fi Networks use Radio Technologies to transmit & receive data at high speed :

- IEEE 802.11b, a,g (Gen 3)
- IEEE 802.11 n (Gen 4)
- IEEE 802.11 ac (Gen 5)
- IEEE 802.11 ax (Gen 6)



IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

- **802.11** – This pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a** – This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS. **More expensive and not compatible with 802.11b**
- **802.11b** – The 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g** – This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band. Compatible with ‘b’

IEEE 802.11n

Introduced in 2009, this version had slow initial adoption. 802.11n operates on both 2.4GHz and 5GHz, as well as supporting multi-channel usage. Each channel offers a maximum data rate of 150Mbps, which means the standard's maximum data rate is 600Mbps.

IEEE 802.11ac

The ac standard is what you will find most wireless devices using at the time of writing. Initially released in 2014, ac drastically increases the data throughput for Wi-Fi devices up to a maximum of 1,300 megabits per second. Furthermore, ac adds MU-MIMO support, additional Wi-Fi broadcast channels for the 5GHz band, and support for more antennas on a single router.

IEEE 802.11ax

Next up for your router and your wireless devices is the ax standard. As ax completes its rollout, you will have access to theoretical network throughput of 10Gbps—around a 30-40 percent improvement over the ac standard. Furthermore, wireless ax will increase network capacity by adding broadcast subchannels, upgrading MU-MIMO, and allowing more simultaneous data streams.

ELEMENT OF A Wi-Fi NETWORK



Access point



Adapters



PCI cards that accept wireless PC cards



External USB wireless NICs

× Antennas come in all shapes and styles:

+ Omni-directional:

× Vertical Whip

× Ceiling mount

+ Directional:

× Yagi (“Pringles can”)

× Wall mounted panel

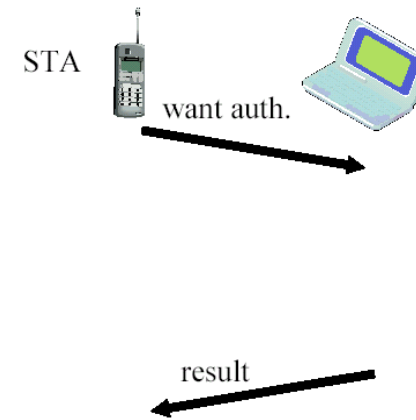
× Parabolic dish



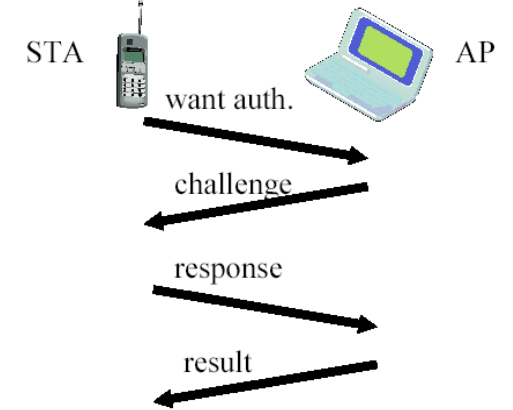
HOW A Wi-Fi NETWORK WORKS?

- Basic concept is same as Walkie talkies.
- A Wi-Fi hotspot is created by installing an access point to an internet connection.
- An access point acts as a base station.
- When Wi-Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.
- A single access point can support up to 30 users and can function within a range of 100 – 150 feet indoors and up to 300 feet outdoors.
- Many access points can be connected to each other via Ethernet cables to create a single large network.

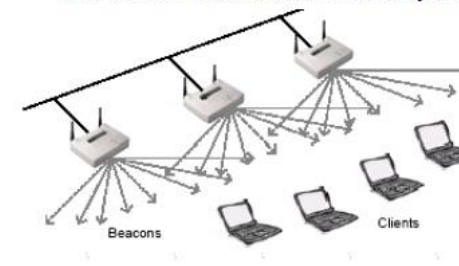
Open System Authentication



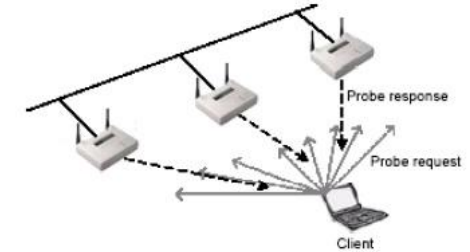
Shared Key Authentication



1. Scanning is the first step for the MC (Mobile Clients) to join an APs network.
2. In the case of passive scanning the client just waits to receive a Beacon Frame from the AP
3. MC (Mobile Clients) searching for a network by just listens for beacons until it finds a suitable network to join.



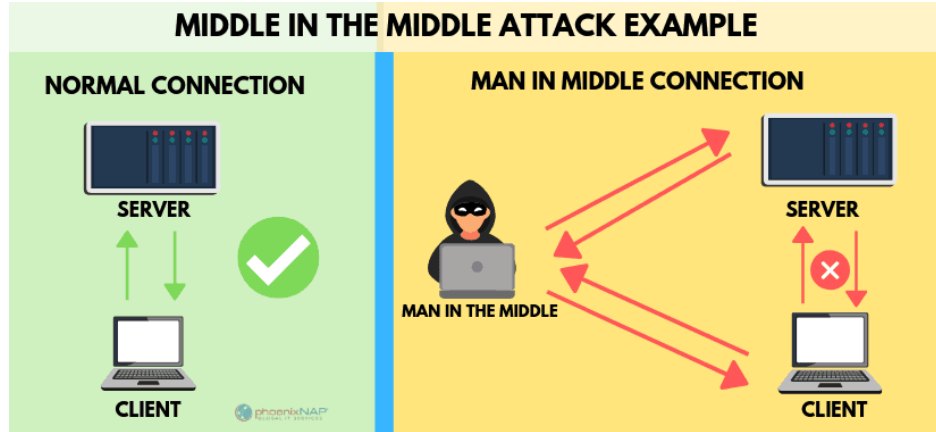
Passive Scan



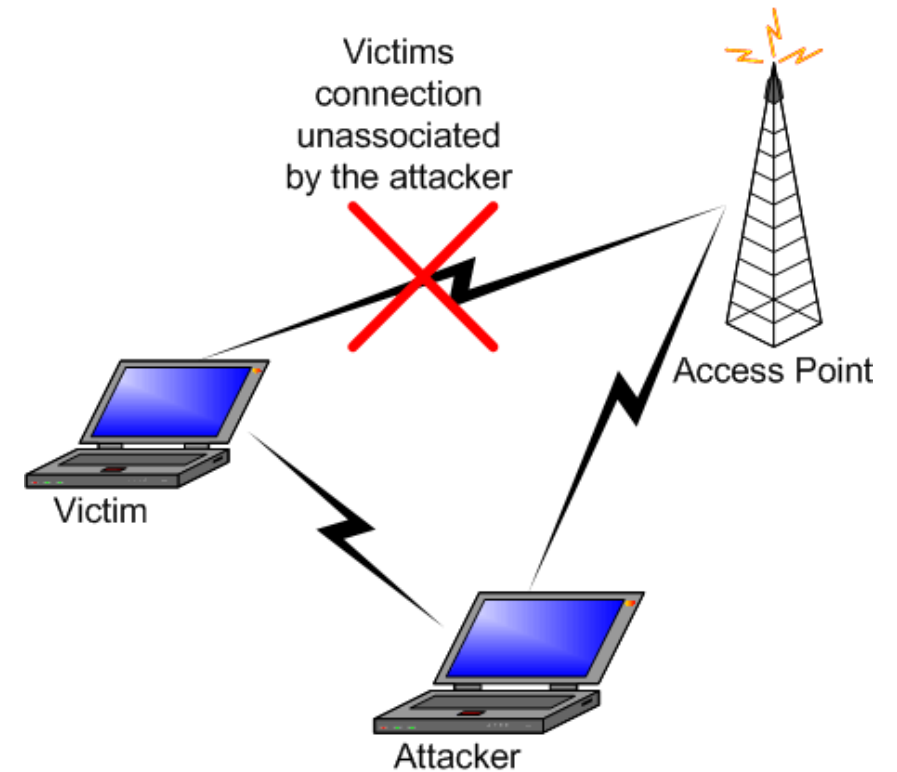
Active Scan

1. The MC (Mobile Clients) tries to locate an AP by transmitting Probe Request Frames, and waits for Probe Response from the AP.
2. The probe request frame can be a directed or a broadcast probe request.
3. The probe response frame from the AP is similar to the beacon frame.
4. Based on the response from the AP, the client makes a decision about connecting to the AP

MITM Attack (Man In the Middle)

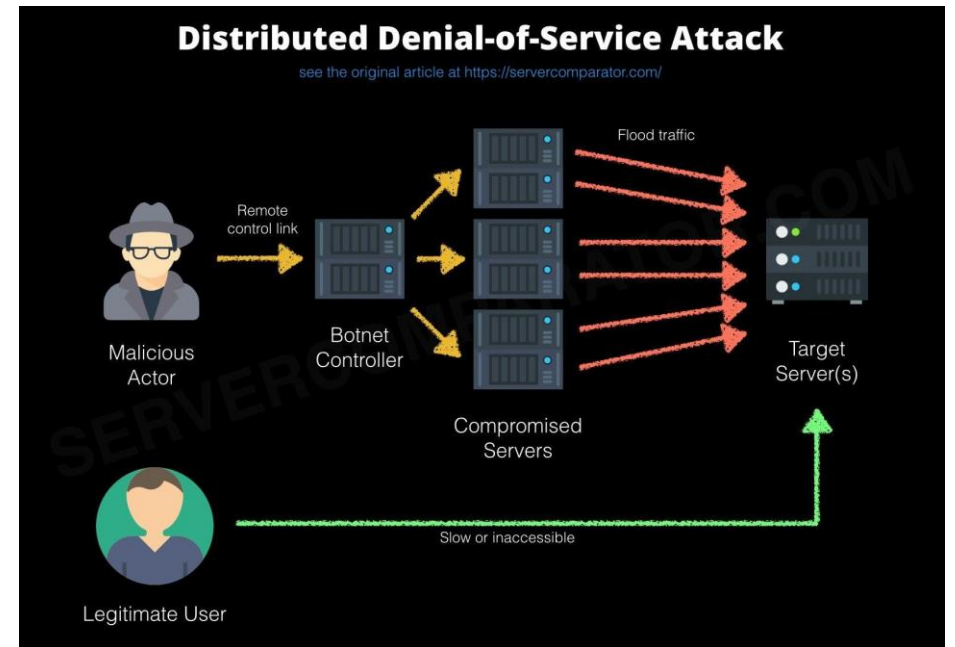


1. Attacker spoofs a disassociate message from the victim
2. The victim starts to look for a new access point, and the attacker advertises his own AP on a different channel, using the real AP's MAC address
3. The attacker connects to the real AP using victim's MAC address



Denial of Service

- Attack on transmission frequency used
 - Frequency jamming
 - Not very technical, but works
- Attack on MAC layer
 - Spoofed deauthentication / disassociation messages
 - can target one specific user
- Attacks on higher layer protocol (TCP/IP protocol)
 - SYN Flooding



Malicious WiFi Hotspots

Any malicious attacker can set up a hidden hotspot and name it whatever they want. While you browse, your traffic is recorded and later analyzed for any sensitive information that may prove useful in compromising your accounts.

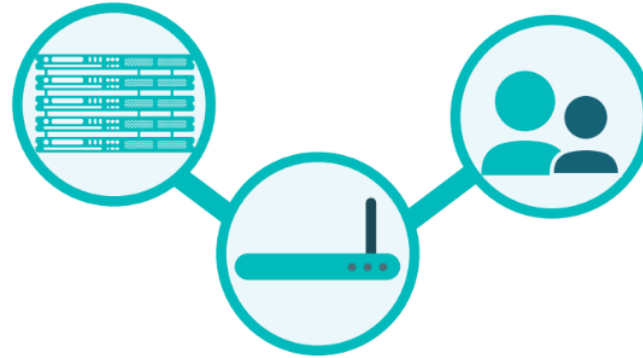


Wi-Fi Security



The requirements for Wi-Fi network security can be broken down into two primary components:

- Authentication
 - User Authentication
 - Server Authentication
- Privacy





Authentication

- Keeping unauthorized users off the network
- User Authentication
 - Authentication Server is used
 - Username and password
 - Risk:
 - Data (username & password) send before secure channel established
 - Prone to passive eavesdropping by attacker
 - Solution
 - Establishing a encrypted channel before sending username and password





Wi-Fi Security Techniques

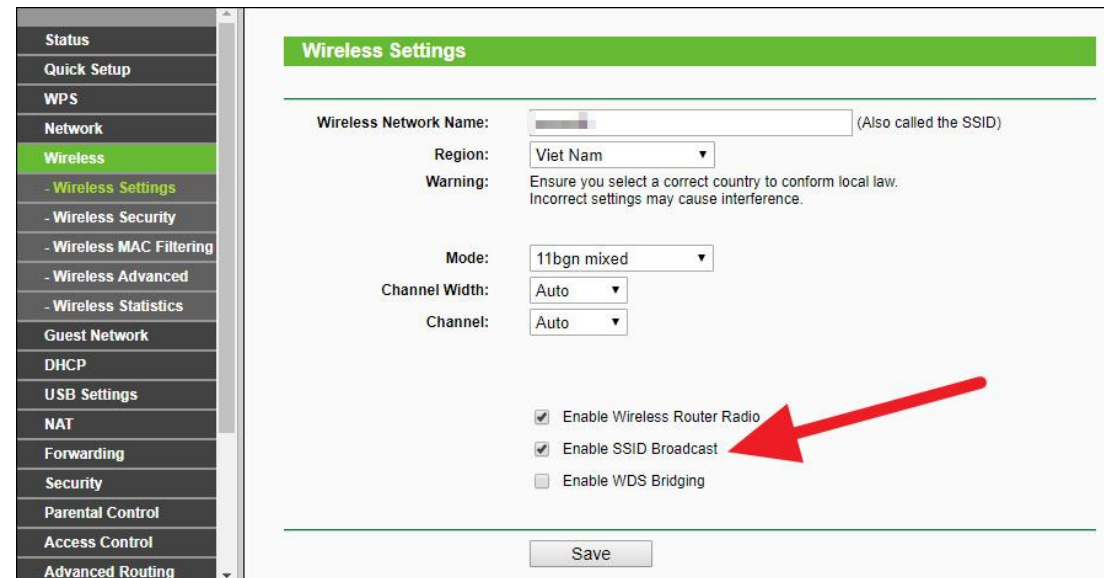
- Service Set Identifier (SSID)
- Wired Equivalent Privacy (WEP)
- 802.1X Access Control
- Wireless Protected Access (WPA)
- IEEE 802.11i





Service Set Identifier (SSID)

- SSID is used to identify an 802.11 network
- It can be pre-configured or advertised in beacon broadcast
- It is transmitted in clear text
 - Provide very little security

A screenshot of a web-based configuration interface for wireless settings. On the left is a vertical navigation menu with items like Status, Quick Setup, WPS, Network, Wireless (highlighted), Wireless Settings, Wireless Security, Wireless MAC Filtering, Wireless Advanced, Wireless Statistics, Guest Network, DHCP, USB Settings, NAT, Forwarding, Security, Parental Control, Access Control, and Advanced Routing. The main content area is titled 'Wireless Settings' and contains several configuration options: 'Wireless Network Name' (a text input field with a placeholder and a note '(Also called the SSID)'), 'Region' (a dropdown menu set to 'Viet Nam' with a warning message below it), 'Mode' (a dropdown menu set to '11bgn mixed'), 'Channel Width' (a dropdown menu set to 'Auto'), and 'Channel' (a dropdown menu set to 'Auto'). At the bottom of the settings are three checkboxes: 'Enable Wireless Router Radio' (checked), 'Enable SSID Broadcast' (checked, with a red arrow pointing to it), and 'Enable WDS Bridging' (unchecked). A 'Save' button is located at the bottom right of the settings area.



Wired Equivalent Privacy (WEP)

- Provide same level of security as by wired network
- Original security solution offered by the IEEE 802.11 standard
- Uses RC4 encryption with pre-shared keys and 24 bit initialization vectors (IV)
- key schedule is generated by concatenating the shared secret key with a random generated 24-bit IV
- 32 bit ICV (Integrity check value)
- No. of bits in keyschedule is equal to sum of length of the plaintext and ICV

4. Click on the button next to WEP

WEP prevents unintentional connections to your wireless network, see Advanced Security Settings.

WEP Off

5. Select a WEP Key

NOTE: - To create a 60/40 WEP Hex Key, you need to enter a 13 digit hexadecimal number from 0-9. Sample HEX WEP Key: 0FB310FF28

Select a WEP Key:

Key Code: 0 Digits left

6. Turn WPS ON





Wired Equivalent Privacy (WEP) (cont.)

- 64 bit preshared key-WEP
- 128 bit preshared key-WEP2
- Encrypt data only between 802.11 stations. once it enters the wired side of the network (between access point) WEP is no longer valid
- Security Issue with WEP
 - Short IV
 - Static key

The screenshot shows a 'Wireless Security' configuration window. The 'Wireless Security' dropdown is set to 'WEP'. The 'Authentication Type' is set to 'Shared Key'. The 'Key Select' dropdown is set to 'Key2'. The 'Key 1' field contains the hexadecimal string '147ac82d852c2e483bd735a26' and is set to '128 bit'. The 'Key 2' field contains the text 'ILoveMyFamily' and is also set to '128 bit'. The 'Key 3' and 'Key 4' fields are empty and are set to '64 bit'. A legend at the bottom indicates that 64-bit keys can be 5 text or 10 hexadecimal digits, 128-bit keys can be 13 text or 26 hexadecimal digits, and 256-bit keys can be 29 text or 58 hexadecimal digits. 'save' and 'reset' buttons are at the bottom.

Key	Value	Length
Key 1	147ac82d852c2e483bd735a26	128 bit
Key 2	ILoveMyFamily	128 bit
Key 3		64 bit
Key 4		64 bit

*WEP keys:
64 bit (5 text or 10 hexadecimal digits)
128 bit (13 text or 26 hexadecimal digits)
256 bit (29 text or 58 hexadecimal digits)





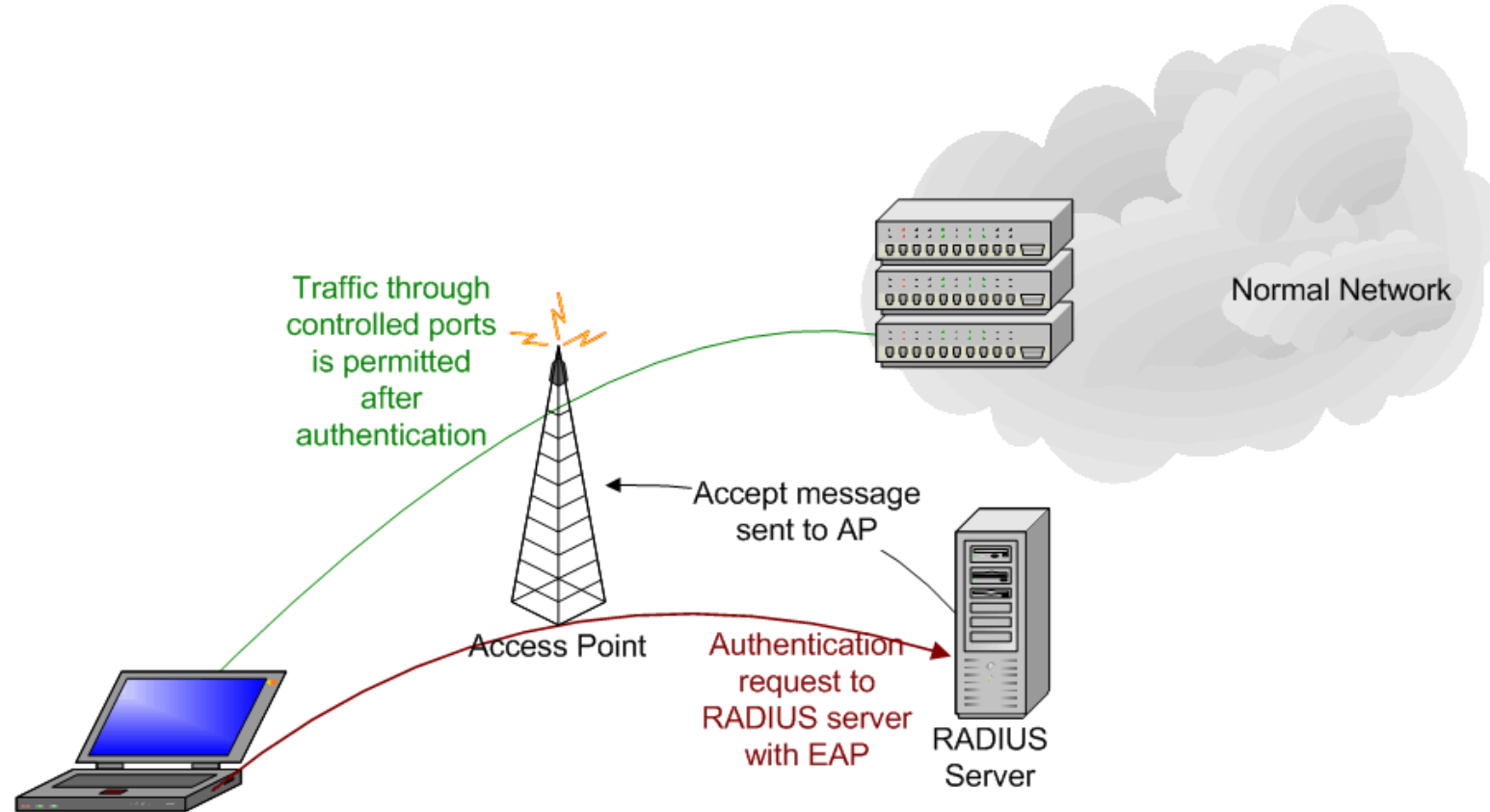
802.1x Access Control

- Designed as a general purpose network access control mechanism
 - Not Wi-Fi specific
- Authenticate each client connected to AP (for WLAN) or switch port (for Ethernet)
- Authentication is done with the RADIUS server, which "tells" the access point whether access to controlled ports should be allowed or not
 - AP forces the user into an unauthorized state
 - user send an Extensible Authentication Protocol (EAP) start message
 - AP return an EAP message requesting the user's identity
 - Identity send by user is then forwarded to the authentication server by AP
 - Authentication server authenticate user and return an accept or reject message back to the AP
 - If accept message is return, the AP changes the client's state to authorized and normal traffic flows





802.1x Access Control





Wireless Protected Access

- WPA is a specification of standard based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN system.
- User Authentication
 - 802.1x
 - EAP
- TKIP (Temporal Key Integrity Protocol) encryption
 - RC4, dynamic encryption keys (session based)
 - 48 bit IV
 - per packet key mixing function
 - Fixes all issues found from WEP
- Uses Message Integrity Code (MIC) Michael
 - Ensures data integrity
- Old hardware should be upgradeable to WPA

The screenshot shows a web-based wireless settings page. On the left is a sidebar menu with 'Wireless' selected. The main content area is titled 'Wireless Settings' and includes the following fields and options:

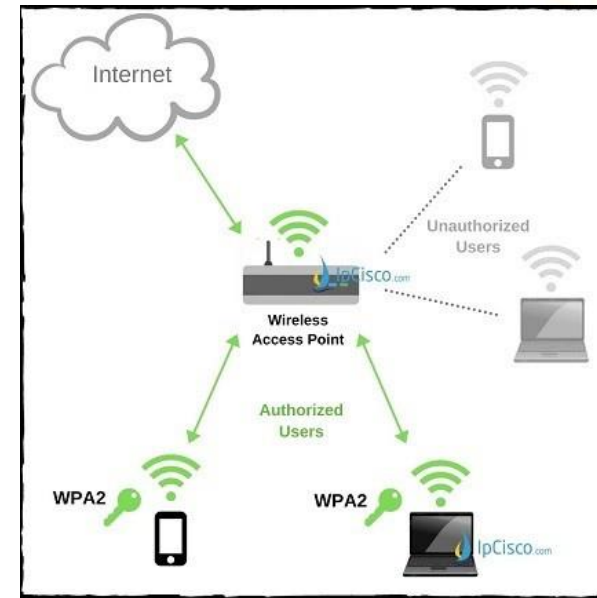
- Enable Wireless Radio:**
- Network Name (SSID):** wifi-settings.com Hide SSID
- Security:** WPA/WPA2-Personal (Recommended) (1)
- Version:** Auto WPA-PSK WPA2-PSK (2)
- Encryption:** Auto TKIP AES (3)
- Password:** 7239846De1
- Mode:** 802.11b/g/n/ax mixed
- Channel Width:** 40MHz
- Channel:** 1
- Transmit Power:** Low Middle High (4)
- Airtime Fairness Feature:** Enable Airtime Fairness
- Save:** A blue button at the bottom right.

Red callout boxes with numbers 1, 2, 3, and 4 are placed over the Security dropdown, the WPA2-PSK radio button, the AES radio button, and the High transmit power radio button, respectively. A red arrow points from callout 4 to the Save button.



Wireless Protected Access (WPA)

- WPA comes in two flavors
 - WPA-PSK
 - use pre-shared key
 - For SOHO environments
 - Single master key used for all users
 - WPA Enterprise
 - For large organization
 - Most secure method
 - Unique keys for each user
 - Separate username & password for each user



Wireless Network:	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled
Network Name (SSID):	<input type="text" value="HOME-D12F"/>
Mode:	802.11 b/g/n ▼
Security Mode:	WPA2-PSK (AES) ▼
Channel Selection:	Open (risky) WEP 64 (risky) WEP 128 (risky) WPA-PSK (TKIP) WPA-PSK (AES) WPA2-PSK (TKIP) WPA2-PSK (AES)
Channel:	
Network Password:	<input type="password" value="WPA2-PSK (AES)"/> WPAWPA2-PSK (TKIP/AES) (recommended)
Show Network Password:	<input checked="" type="checkbox"/>



- The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

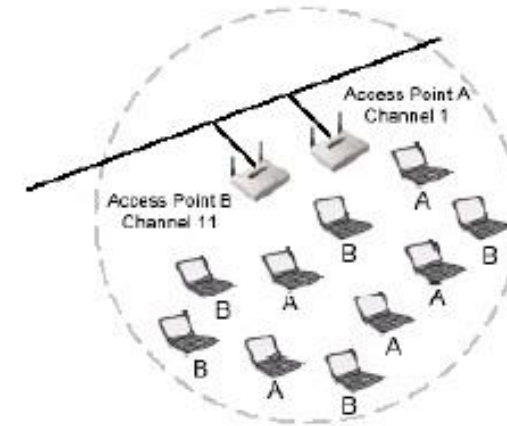
WiFi Protected Access 2 (WPA2)

- A year later, in 2004, WiFi Protected Access 2 became available. WPA2 has stronger security and is easier to configure than the prior options. The main difference with WPA2 is that it uses the Advanced Encryption Standard (AES) instead of TKIP. AES is able to secure top-secret government information, so it's a good option for keeping a personal device or company WiFi safe.

LB & RA

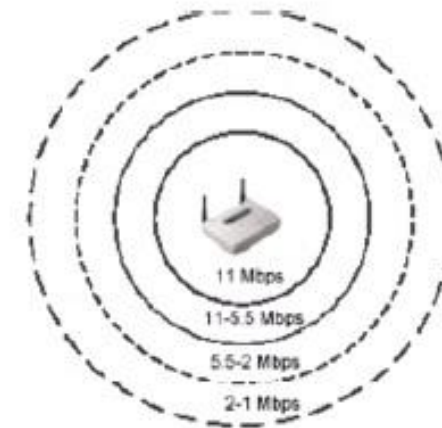
❖ Load Balancing

- Important issue in areas of heavy traffic
- In multicell structure having heavy traffic, several co-located APs can cover the same region to increase the throughput.
- The clients having load balancing functionality configured can automatically associate with the AP that is less loaded and provides the best quality of service.



❖ Rate Adaptation (dynamic rate shifting)

- Speed adjusted dynamically depending on the distance and the signal strength
- As the distance between the AP and the MC (Mobile Client) increases, the signal strength will decrease to a point where the current data rate cannot be maintained .
- when the signal strength decreases the transmitting unit will drop its data rate to the next lower data rate in order to maintain a reasonable SNR.



Wi-Fi APPLICATIONS



- Home
- Small Businesses or SOHO
- Large Corporations & Campuse
- Health Care
- Wireless ISP (WISP)
- Travellers





Gi-Fi TECHNOLOGY

NEXT GENERATION WIRELESS TECHNOLOGY

INTRODUCTION To Gi-Fi

➤ For many years cables ruled the world, optical fibres played a dominant role for its faster transmission but installation of cable caused a greater difficulty and lead to wireless access.

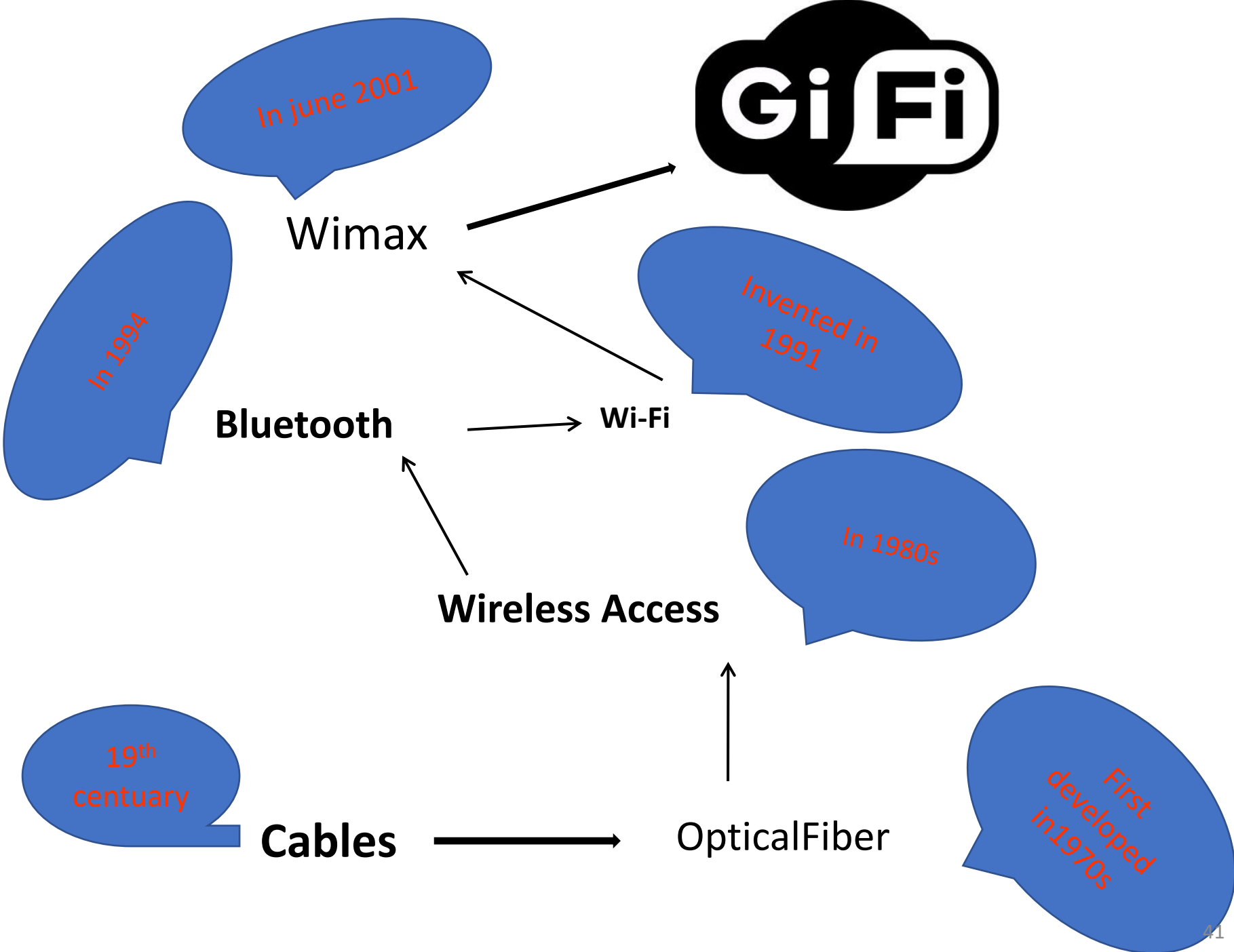
➤ Foremost of this is bluetooth then Wi-Fi followed it. But the mans continuous quest for even better technology led to the introduction of new ,more up-to-date standard for data exchange rate i.e. Gi-Fi.

➤ Wi-Fi(ieee-802.11b) and WiMax(ieee-802.16e) have captured our attention.

➤ As there is no recent developments which transfer data at faster rate, as Video information transfer taking lot of time.

This leads to introduction of Gi-Fi technology it offers some advantages over Wi-Fi, a similar wireless technology.

➤ It was developed at the National Information And Communication Technology Research Center in MELBOURNE,AUSTRALIA.



Comparison of Bluetooth and Wi-Fi with Gi-Fi

characteristics	Bluetooth	Wi-Fi	Gi-Fi
Frequency	2.4GHz	2.4GHz	60GHz
Range	10 meter	100meters	10meters
Primary application	WPAN cable replacement	WLAN Ethernet	Embedded in devices
Data transfer rate	800 Kbps	11Mbps	5Gigabps
Power consumption	5mw	10mw	2mw
Primary devices	Mobile phones,PDA's,consumer electronics,office and industrial devices	Notebooks,desktop computer	Fax,Printer, Cellular phones
Primary uses	Travelling employees,electronics consumers,office ad industrial workers	corporate users	Wireless Home & office appliances ,etc.
Usage location	Anywhere atleast two bluetooth device exist-ideal for roaming outside buildings	Within range of WLAN infrastructure,usually inside a buildings	WPAN Networks
Specification	Bluetooth S&G	IEEE 802.11b,WBCA	IEEE 802.15.3C

What Is Gi-Fi ?

- ❖ Gi-Fi or Gigabit Wireless is the world's first transceiver integrated on a single chip that operates at 60GHz on the CMOS process.
- ❖ Gi-Fi will allow wireless transfer of audio and video data up to 5 gigabits per second.
- ❖ Gi-Fi is ten times the current maximum wireless transfer rate usually within a range of 10 meters.
- ❖ It transmits multiple signals simultaneously across the wireless transmission paths within separate frequencies to avoid interference.

It uses ultra wide band.

Which consists of :

- ❖ High bit rate
- ❖ High security
- ❖ Faster data transmission

Gi-Fi Applications?

1. House hold appliances :

-it makes the wireless home of the future:

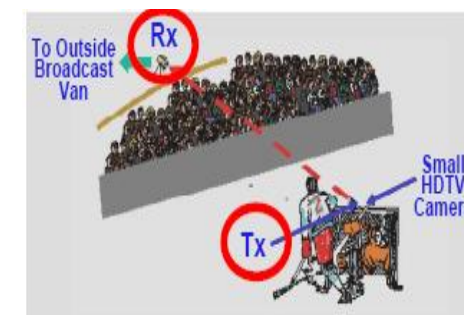
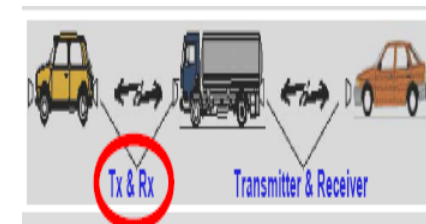
2. Office appliances

3. Video information transfer

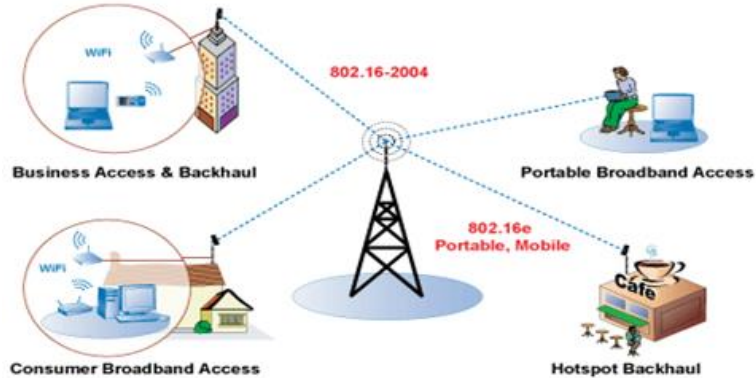
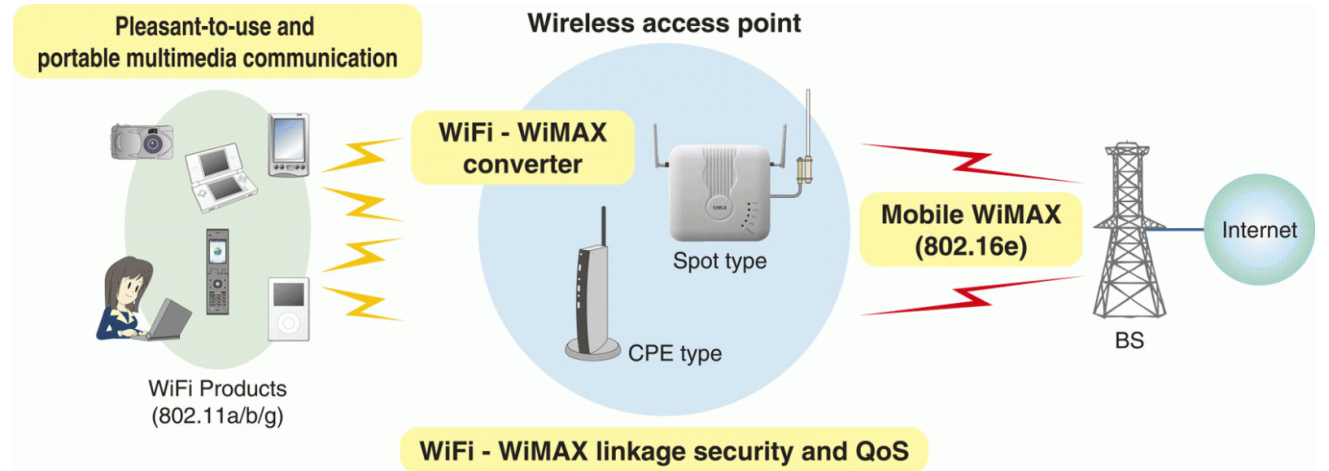
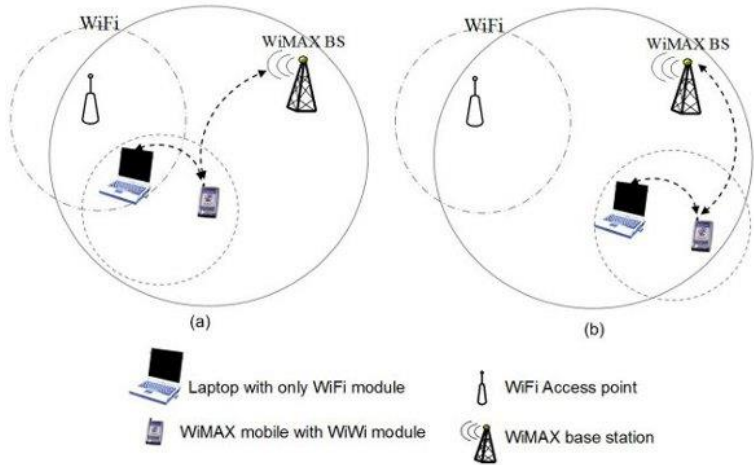


4. Inter-vehicle communication system

5. Broadcasting video signal transmission system in sports stadium



WiFi AND WiMAX AS METRO ACCESS Network



WHAT IS LI – FI ?

- LI-FI is transmission of data through illumination ,sending data through a LED light bulb that varies in intensity faster than human eye can follow

HISTROY

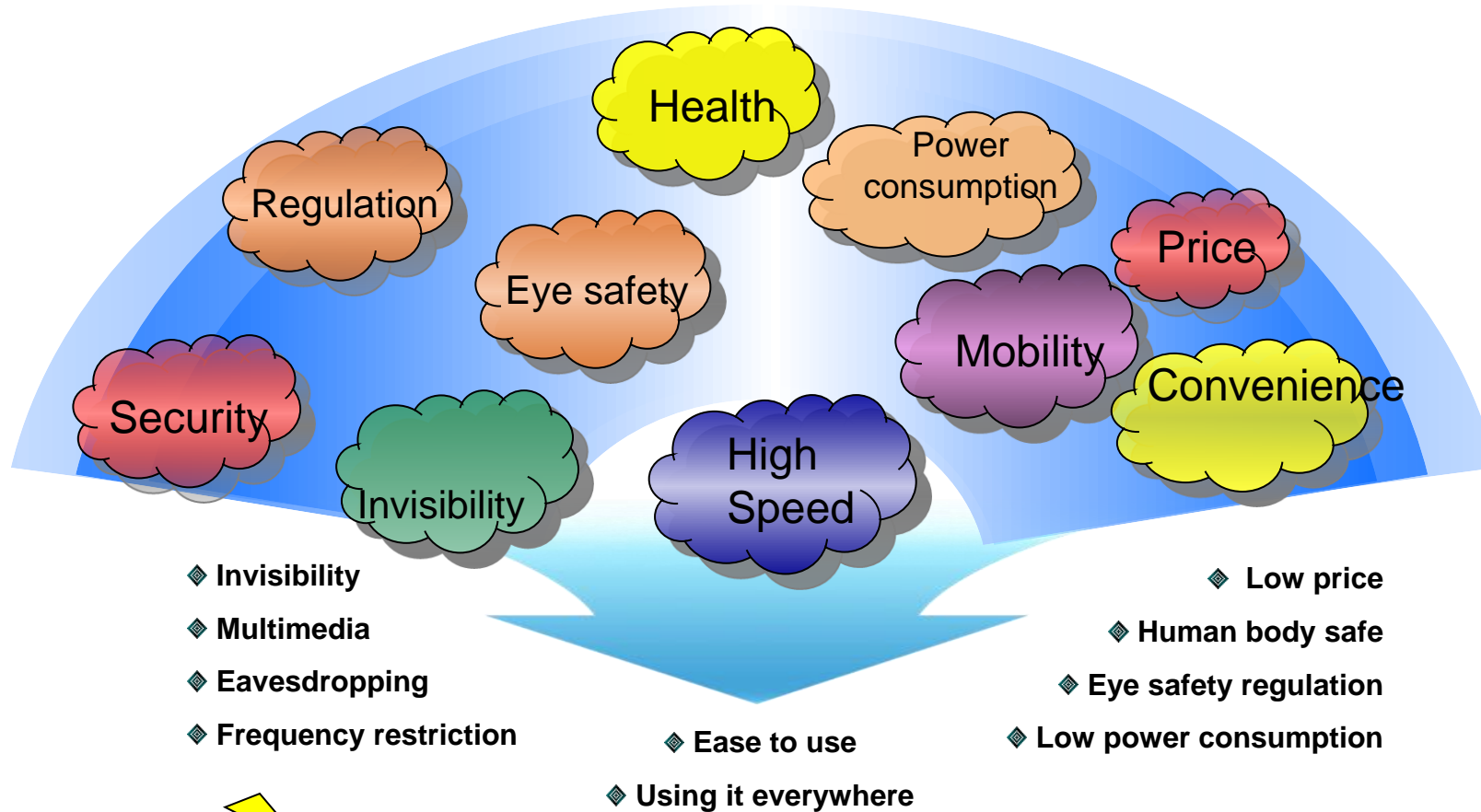
- ❖The technology truly began during the 1990's in countries like Germany, Korea, and Japan where they discovered LED's could be retrofitted to send information. Harald Haas continues to wow the world with the potential to use light for communication



HARALD HASS

<https://www.youtube.com/watch?v=iHWIZsIBj3Q>

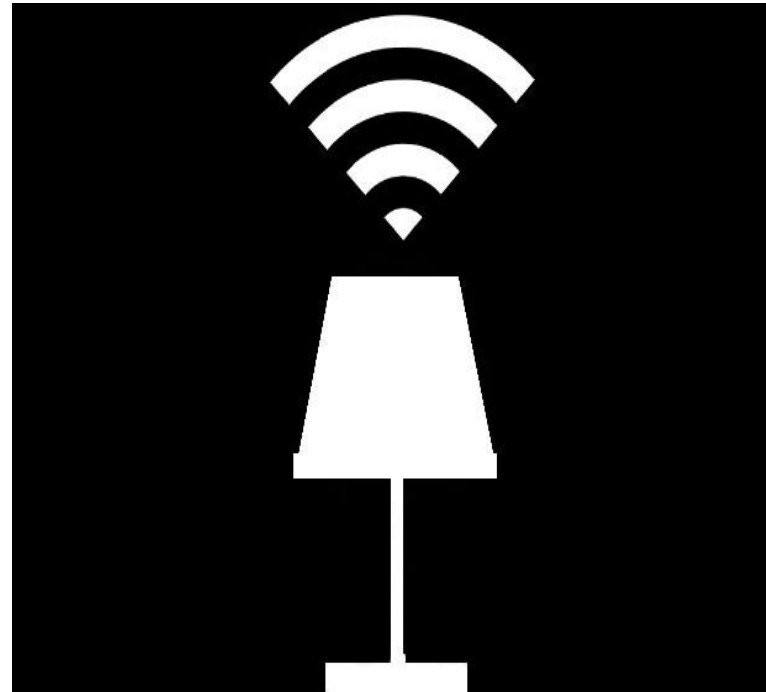
❖ New Idea for the Communication?



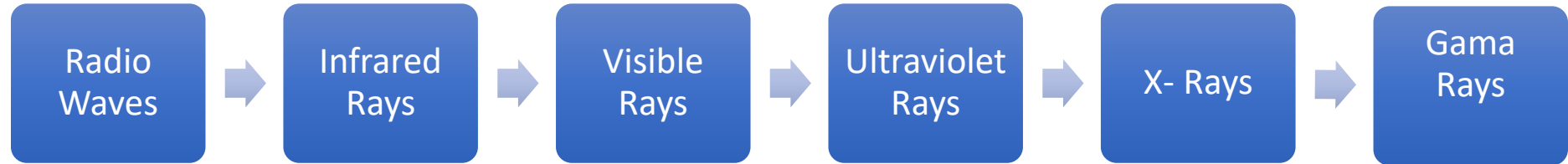
 There is a large range of new opinion on these consideration.

How LI-FI Works ?

❖ operational procedure is very simple, if the led is on, you transmit a digital 1, if its off you transmit a 0. The LEDs can be switched on and off very quickly, which gives nice opportunities for transmitting data. Hence all that us required is some LEDS and a controller that code data into those LEDS.



WHY ONLY VLC

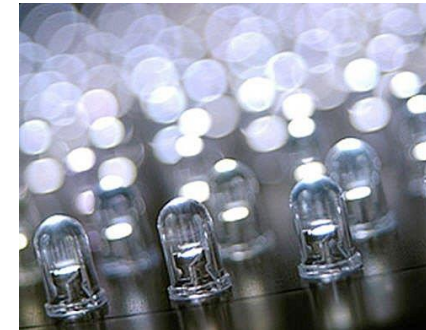


- ❖ Gama rays cant be used as they could be dangerous.
- ❖ X-rays have similar health issues.
- ❖ Ultraviolet light is good for place without people, but other wise dangerous for the human body.
- ❖ Infrared, due to eye safety regulation, can only used with low power.

HENCE WE LEFT WITH THE ONLY THE VISIBLE - LIGHT SPECTRUM.

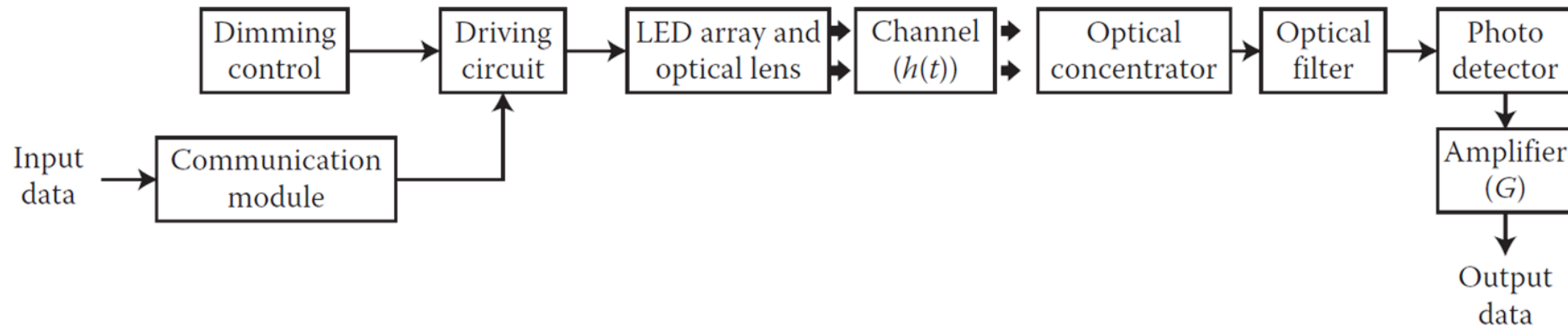
General Lighting Sources

- Incandescent bulb
 - First industrial light source
 - 5% light, 95% heat
 - Few thousand hours of life
- Fluorescent lamp
 - White light
 - 25% light
 - 10,000s hours
- Solid-state light emitting diode (LED)
 - Compact
 - 50% light
 - More than 50,000 hours lifespan



A block diagram of a VLC system

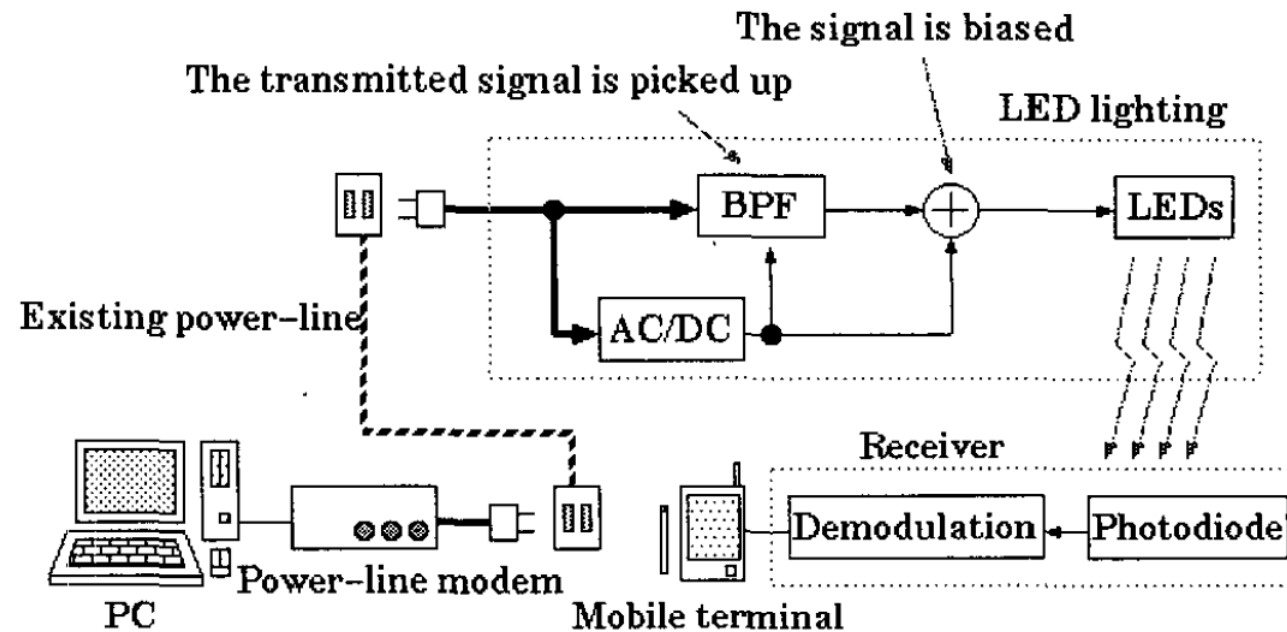
- Precise dimming appears to be challenging for incandescent and gas-discharge lamps
- With LEDs it is quite convenient to accurately control the dimming level
- The illumination requirement is that the illuminance must be 200–1000 lx for a typical office environment



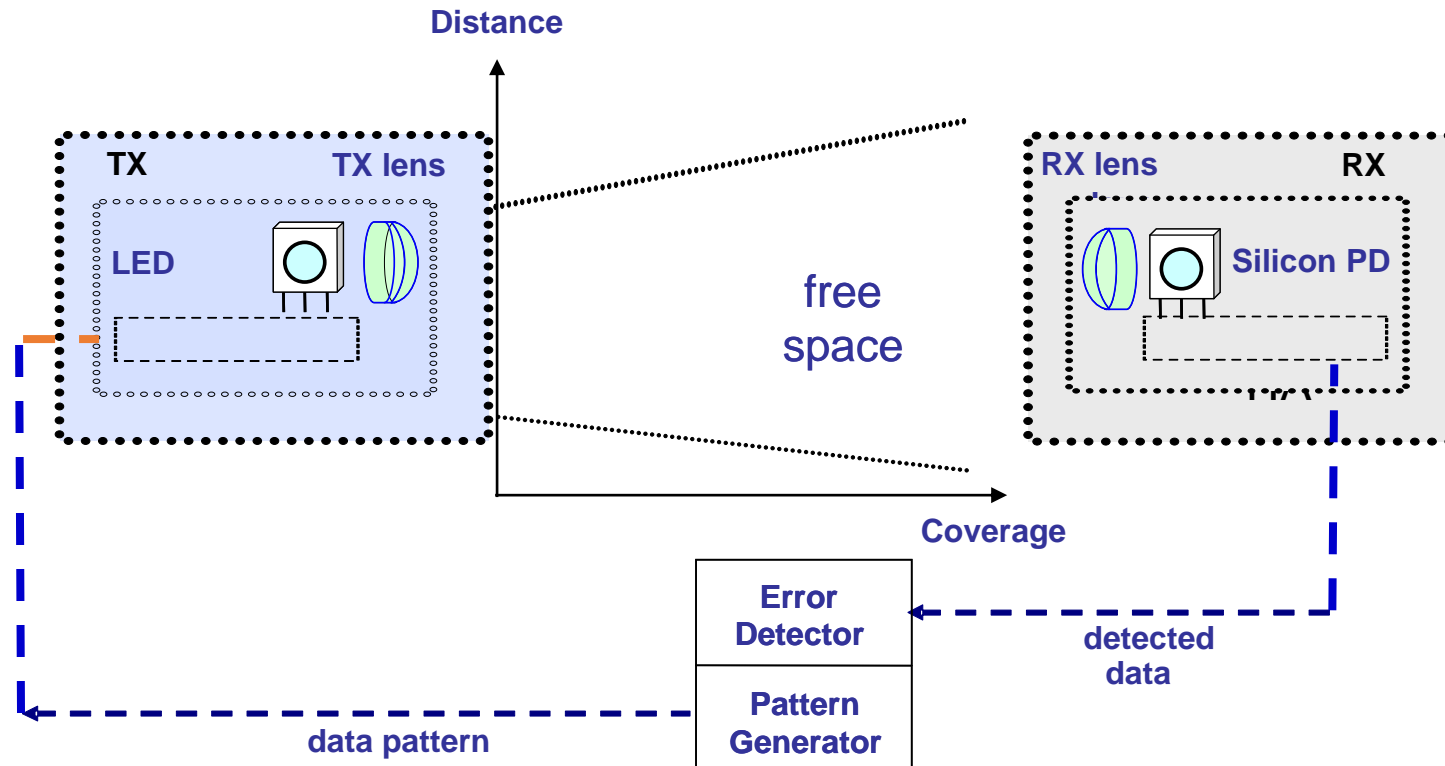
Signal Distribution

Three main options:

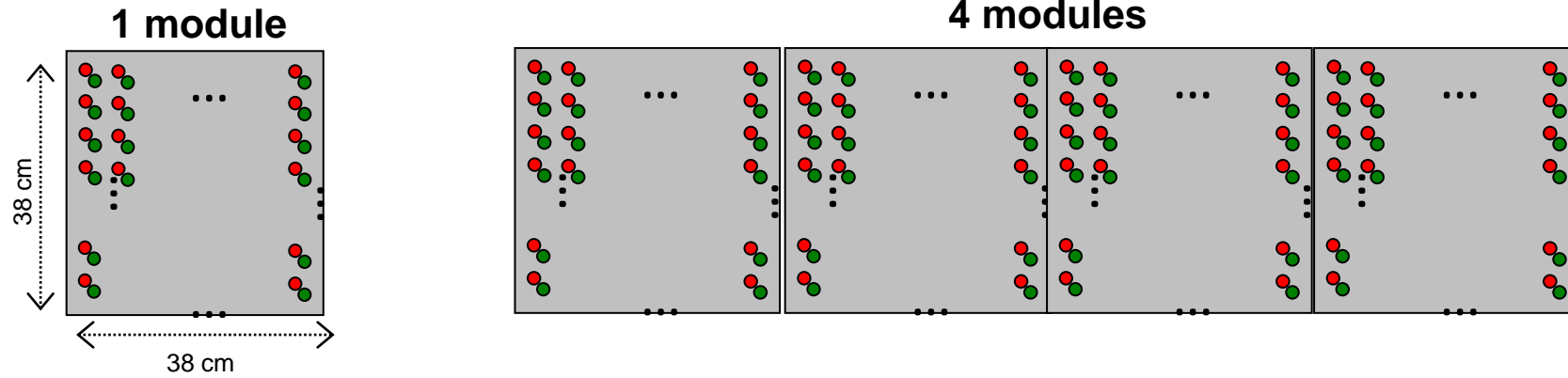
- Electrical network – extension of Internet
- Passive optical network (PON)
- Wireless-over-fiber
- Power-line communication system



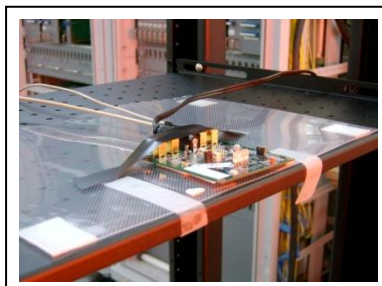
❖ Basic Experimental Setup



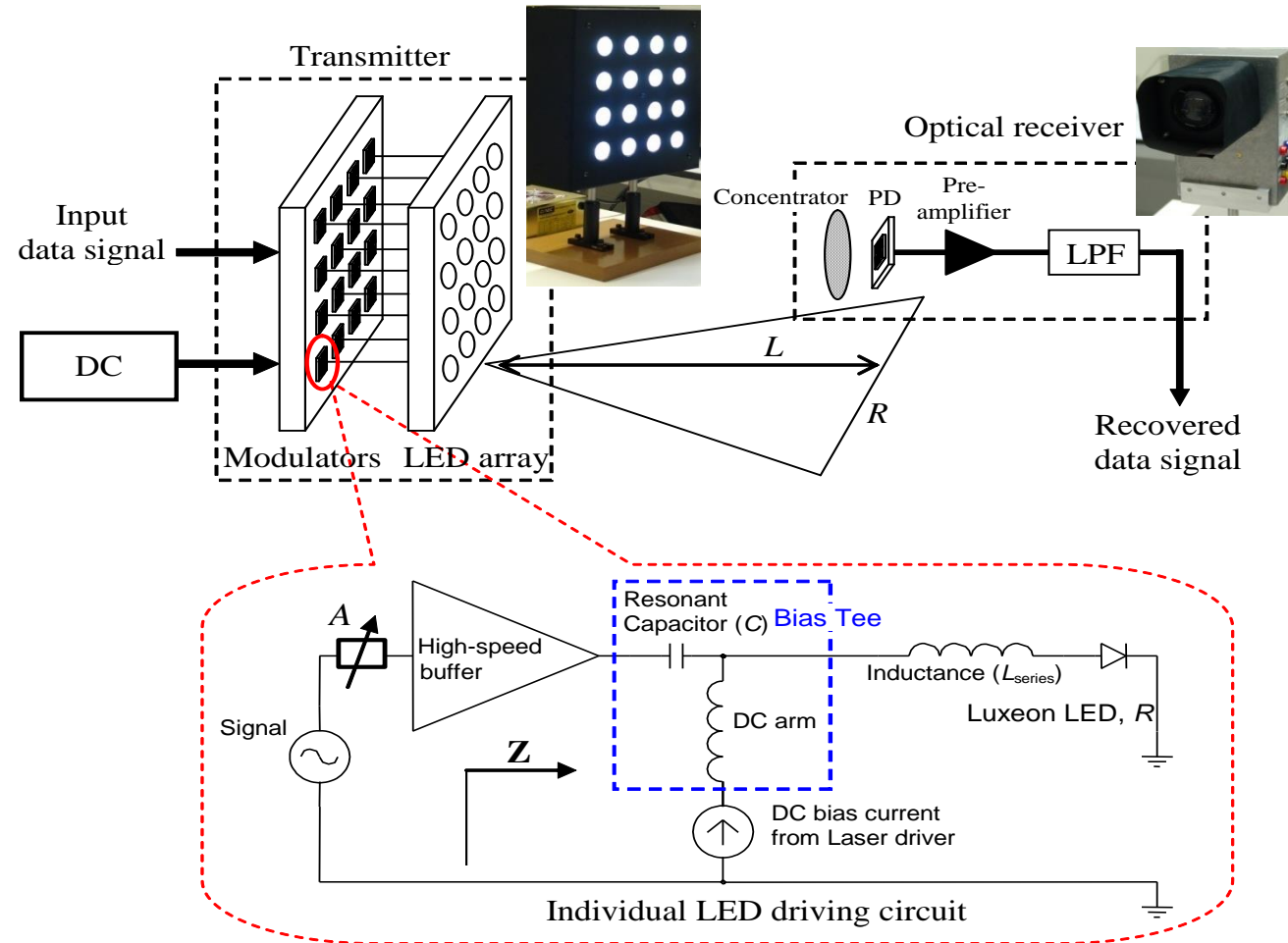
❖ Feasibility Test (visible signboard)



- Red LED : 16 x 16
- Green LED : 16 x 16



VLC Transceivers

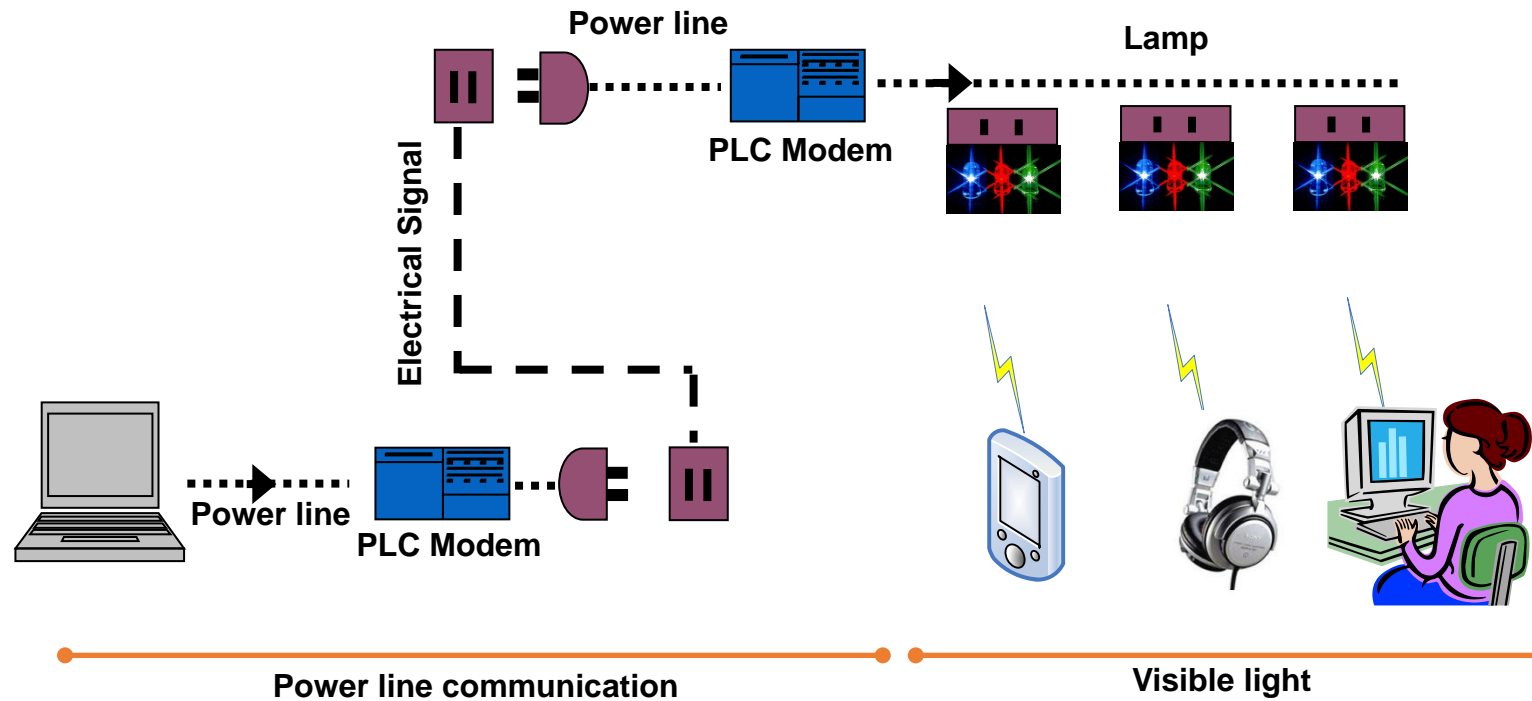


DC current: for illumination (provide sufficient brightness)

Signal: Data for communications

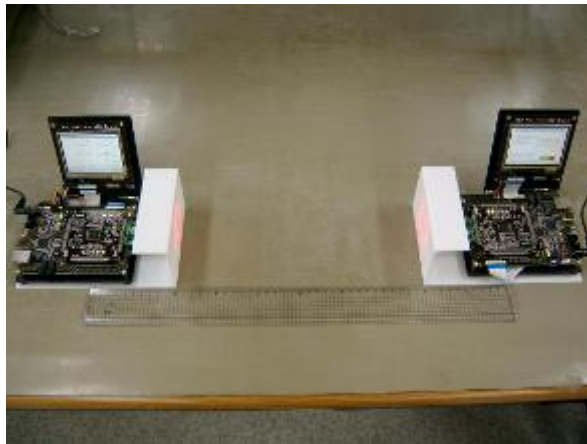
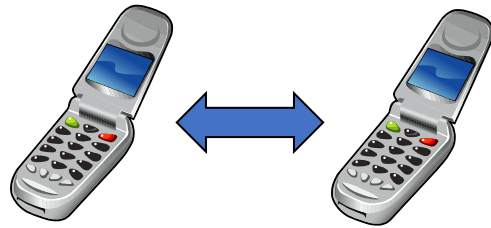
❖ Network Access

- **PLC (Power Line Communication) : other application scenario**
 - A kind of communication system using electric power lines



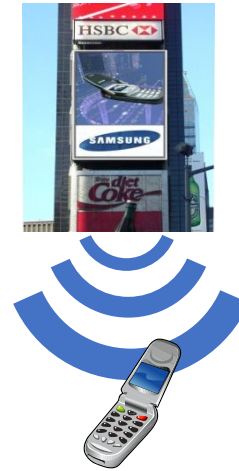
VLC demonstration

Mobile to mobile



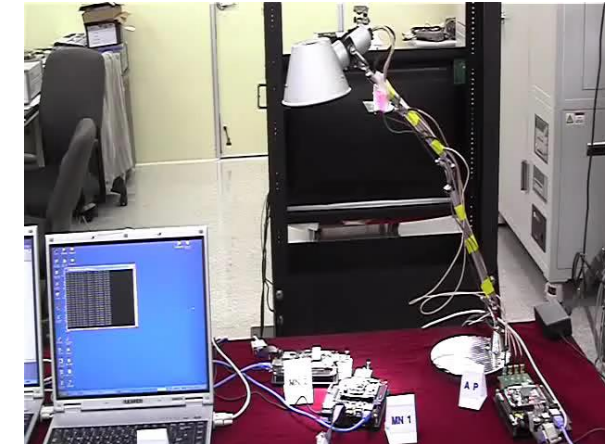
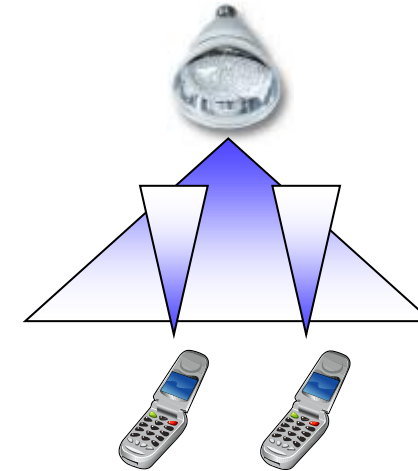
100 Mb/s, 1m
Bidirection

Infra to mobile



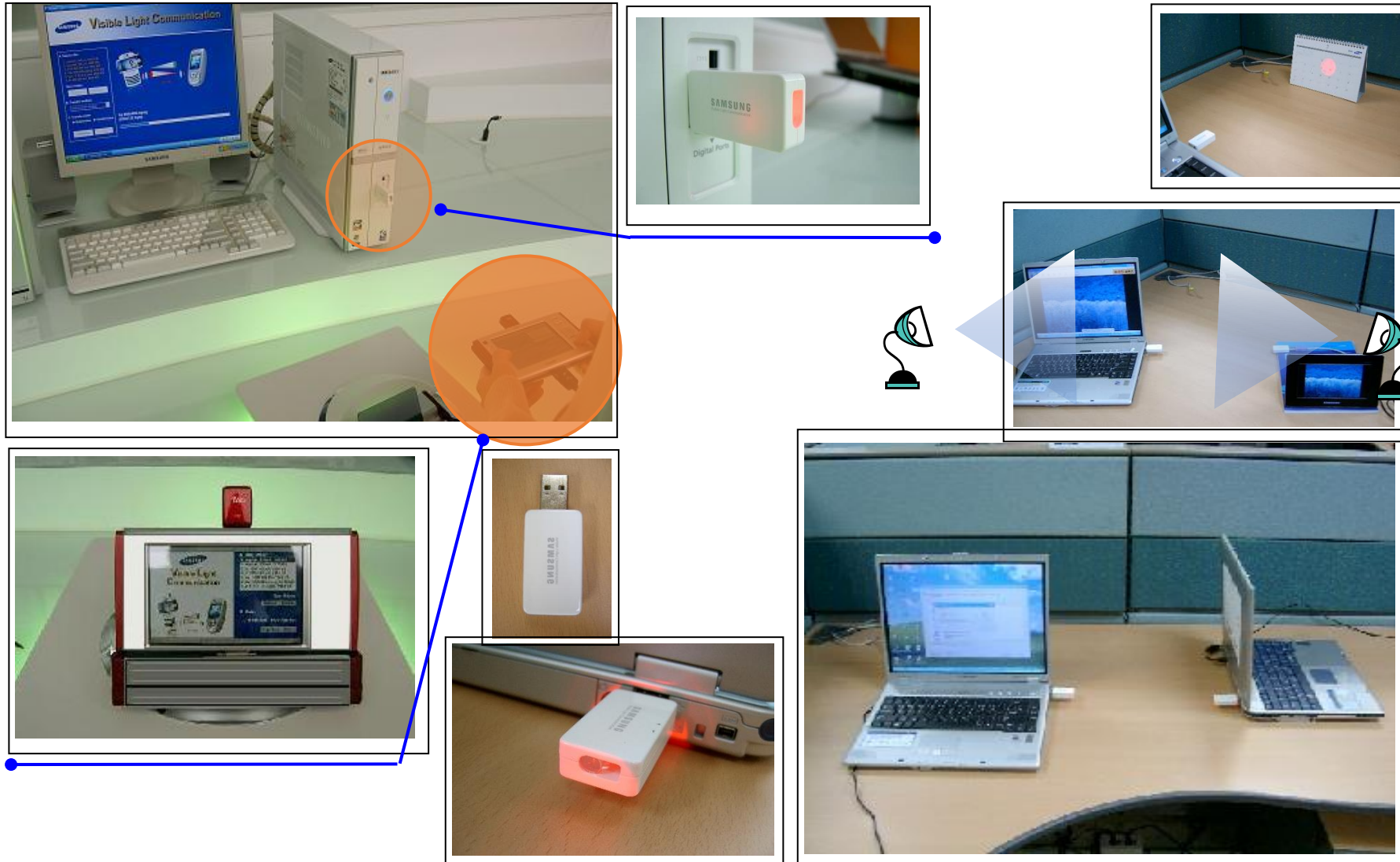
20 Mb/s, 3m
Unidirection

Infra to mobile



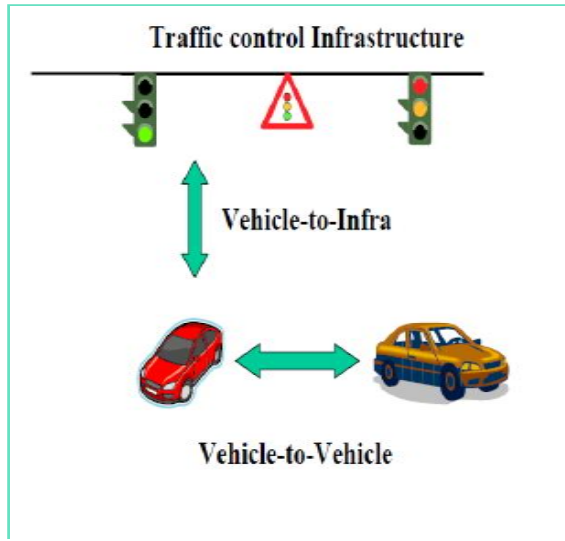
4 Mb/s, 3m
Bidirection

❖ Feasibility Test (PDA-PC/PC-PC visible link)



POTENTIAL APPLICATION OF LI-FI

- Traffic lights can communicate to the car and with each other.
- Cars have LED-based headlights, LED-based cack lights, and cars can communicate with each other and prevent accidents in by exchanging information.



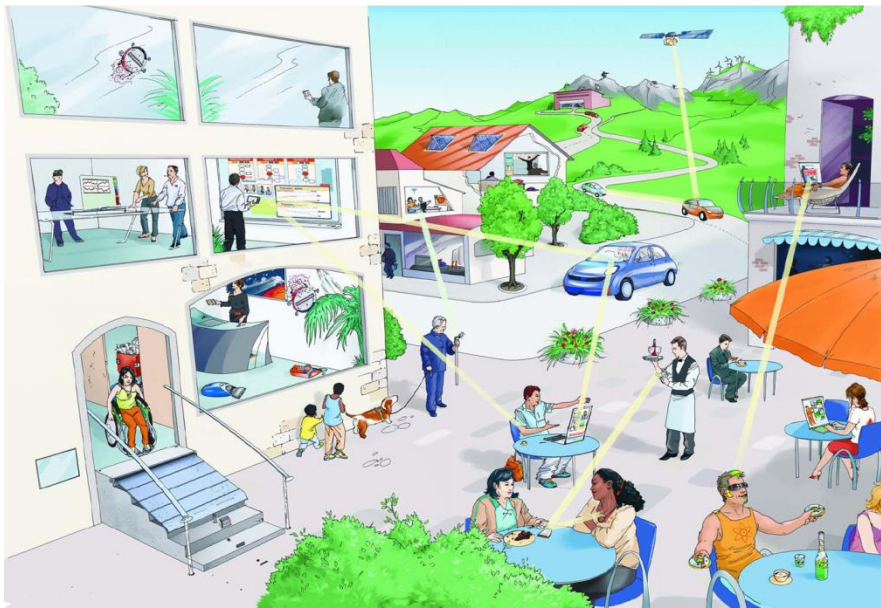
POTENTIAL APPLICATION OF LI-FI

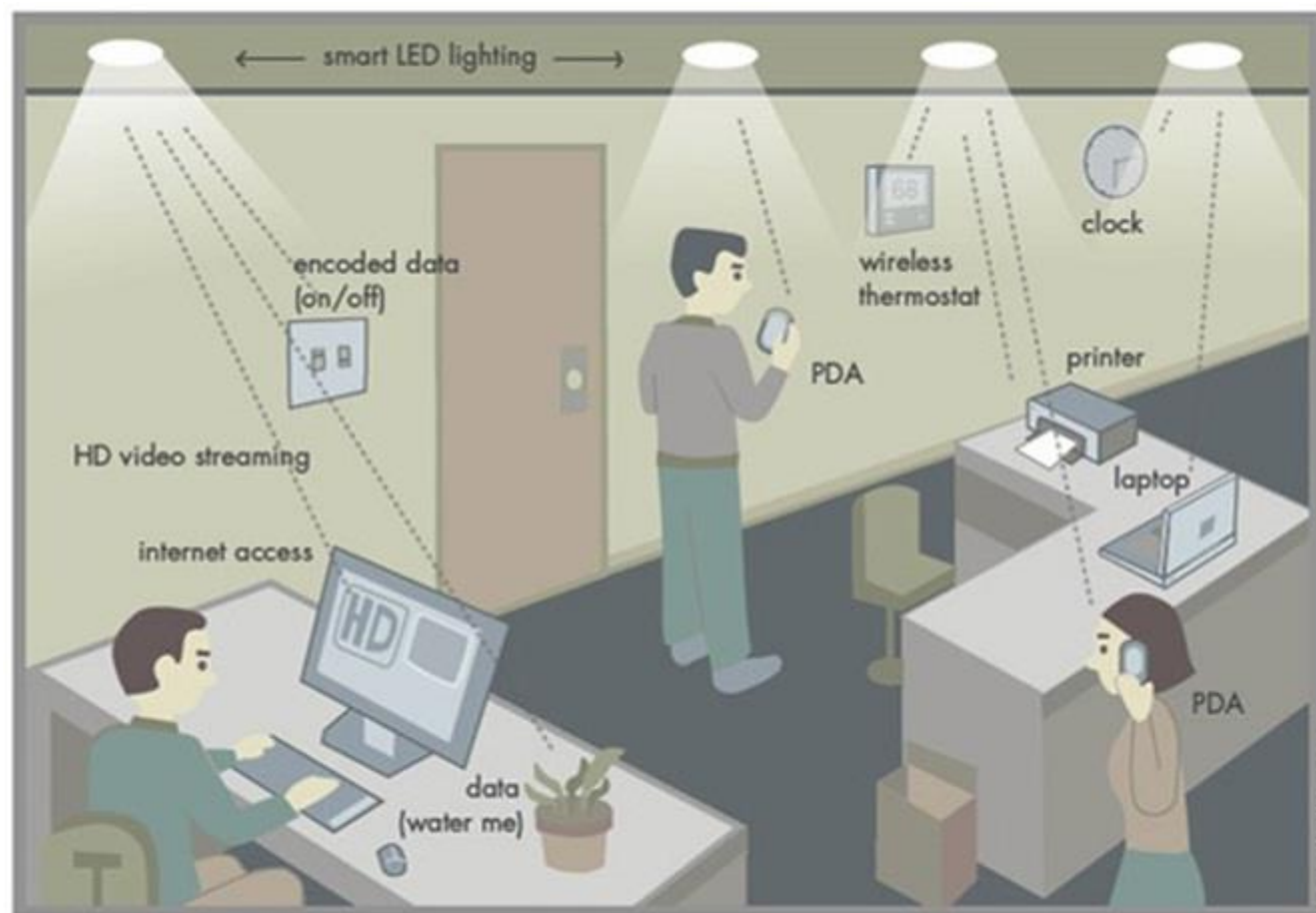
☐ INTRINSICALLY SAFE ENCIRONMENTS

- Visible Light is more safe than RF, hence it can be used in places where RF can't be used such as petrochemical plants , airplanes etc.

☐ PUBLIC INTERNET HOTSPOTS

- There are millions of street lamps deployed around the world.
- Each of these street lamps could be a free access point.





POTENTIAL APPLICATION OF LI-FI

□ ON OCEAN BEDS

- Li-Fi can even work underwater where Wi-Fi fails completely, thereby throwing open endless opportunities for military/navigation operations.



VLC vs. Infrared (IR) and Radio-frequency(RF)

Comparison of VLC, IR and RF Communication Technologies

Property	VLC	IRB	RFB
Bandwidth	Unlimited, 400–700 nm	Unlimited, 800–1600 nm	Regulated and limited
Electromagnetic interference + hazard	No	No	Yes
Line of sight	Yes	Yes	No
Distance	Short	Short to long (outdoor)	Short to long (outdoor)
Security	Good	Good	Poor
Standards	In progress (IEEE 802.15.7 Task Group)	Well developed for indoor (IrDa), In progress for outdoor	Matured
Services	Illumination + communications	Communications	Communications
Noise sources	Sun light + other ambient lights	Sun light + other ambient lights	All electrical/ electronic appliances
Power consumption	Relatively low	Relatively low	Medium
Mobility	Limited	Limited	Good
Coverage	Narrow and wide	Narrow and wide	Mostly wide

Challenges and Solutions

As discussed before, main challenges for indoor VLC systems are

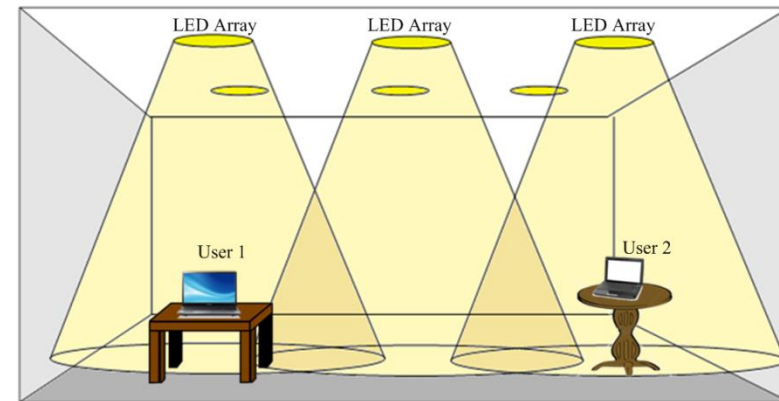
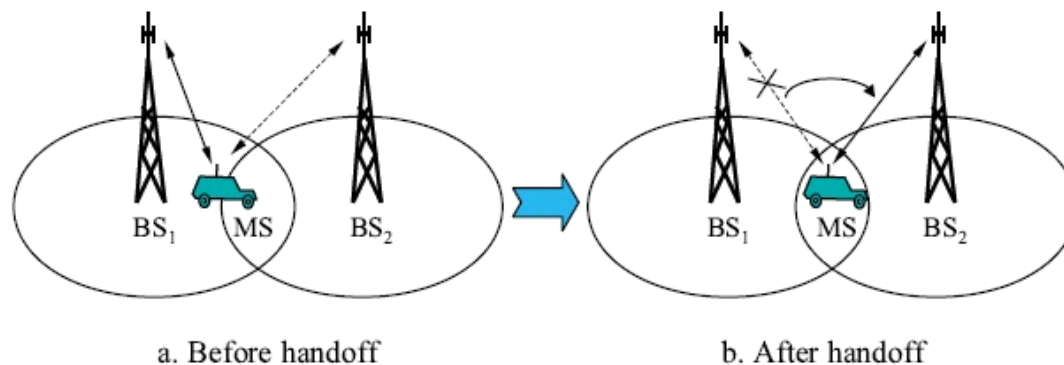
- Connectivity while moving: users need to be connected when they move inside the indoor environment
- Multiuser support: in large areas is vital, many users need to have access to the network at the same time
- Dimming: is an important feature in VLC when communications is integrated with lighting
- Shadowing: happens when the direct paths from user to all sources are blocked

Some solution has been proposed for each one

Challenges and Solutions

Solution for connectivity

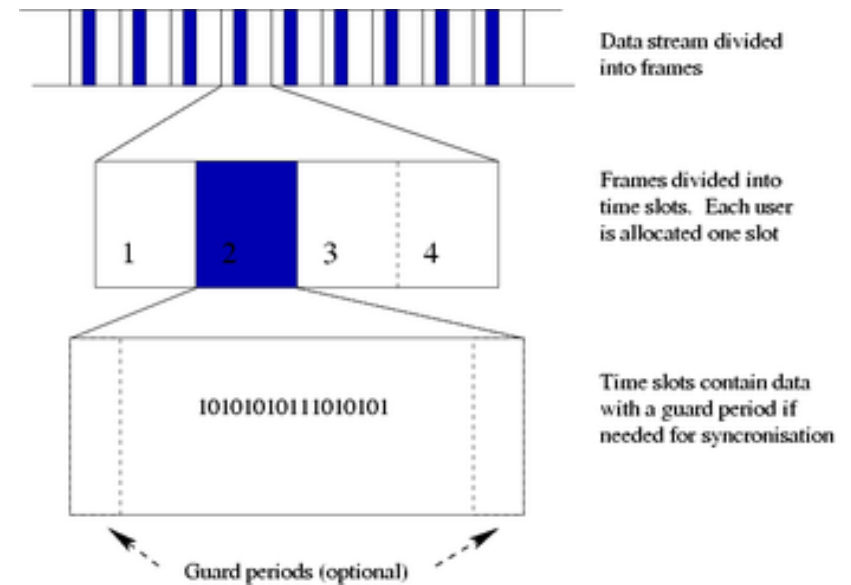
- This problem is similar to the connectivity problem in cellular network when you move from one area of the city to another area while speaking with cell-phone
- The solution is called “handover”, using which the user is transferred from one BS to another
- Handover is done in the area that two BS’s have common coverage
- Similar solution can be used in signal processing domain for VLC
- The user can be transferred from one light source to another in the area that is under the coverage of both



Challenges and Solutions

Solution for multiuser support

- One solution is time division multiplexing (TDM)
- Each frame is divided into equal time slots
- Each user transmit data in one time slot in a predefined order

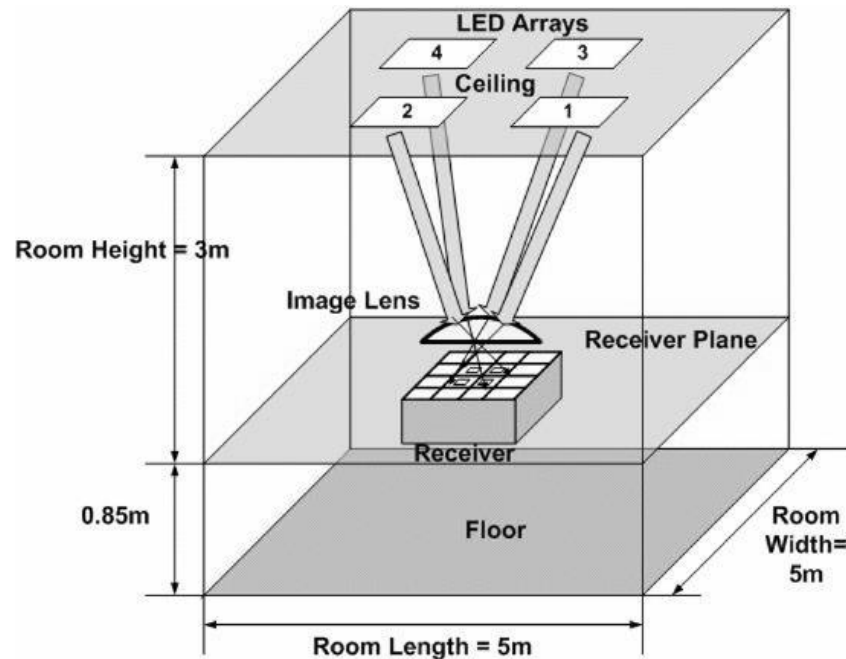


- The other solution is code division multiple access (CDMA)
- Codes are assigned to users
- Each user transmit its data using the assigned signature pattern
- It is used in 3G and 4G cellular networks
- CDMA has been adopted and developed for optical systems
- Optical orthogonal codes (OOC) are used as signature pattern for users

Challenges and Solutions

Solution for multiuser support

- Last solution is spatial multiplexing
- Can use to increase data rate or to add users
- Rely on LED arrays and multiple receivers
- Or can use an imaging receiver (camera)



Challenges and Solutions

Solution for dimming

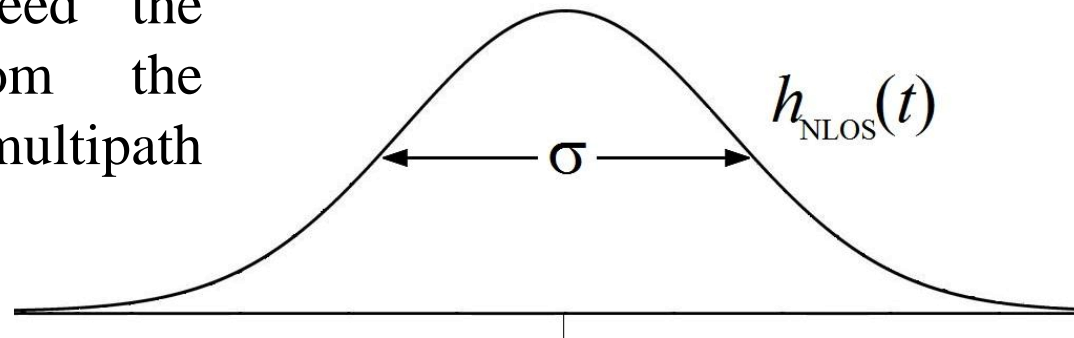
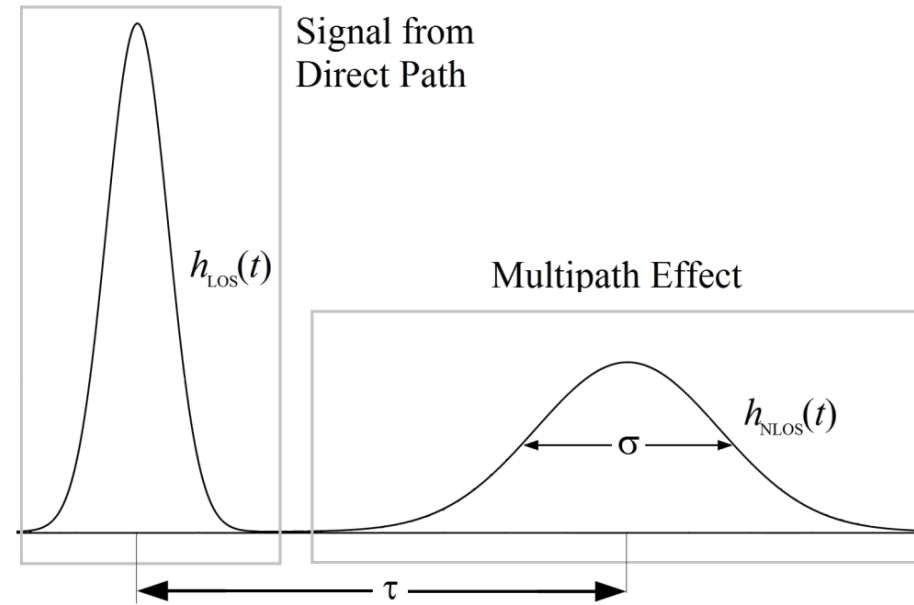
- Two main solutions are proposed for solving dimming problem in VLC systems
- Pulse width modulation (PWM) is combined with other modulation schemes in order to control the duty cycle of the transmitter signal
- By controlling the width of the PWM signaling, the dimming level can be controlled

- The other solution is using modified forms of PPM
- In these schemes multiple pulses are transmitted instead of one pulse
- By controlling and changing the ratio between the number of pulses and the length, the dimming level can be altered

Challenges and Solutions

Solution for shadowing

- As shown before, the impulse response in VLC systems has two parts
- When the line-of-sight (LOS) part (which is received via direct path) is blocked, the impulse response is only the second part
- Then the data can be recovered using the second part which is indeed the received data from the indirect paths (multipath signal)



CONCLUSION

The possibilities are numerous and can be explored further. If this technology can be put into practical use , every bulb can be used something like a Wi-Fi hotspots to transmit wireless data.

