MODULE 2

WIRELESS NETWORKS

Contents

- Wireless network.
- Wireless network Architecture.
- Classification of wireless networks – WBAN, WPAN, WLAN, WMAN, WWAN.
- IEEE 802.11
- IEEE 802.16
- Bluetooth – Standards, Architecture and Services.

Wireless network

Wired network

- Wire as communication
- High data rate
- No mobility

Wireless network

- Radio waves and air as a medium
- Less data rate
- Highly portable
- Mobility

Elements of wireless network

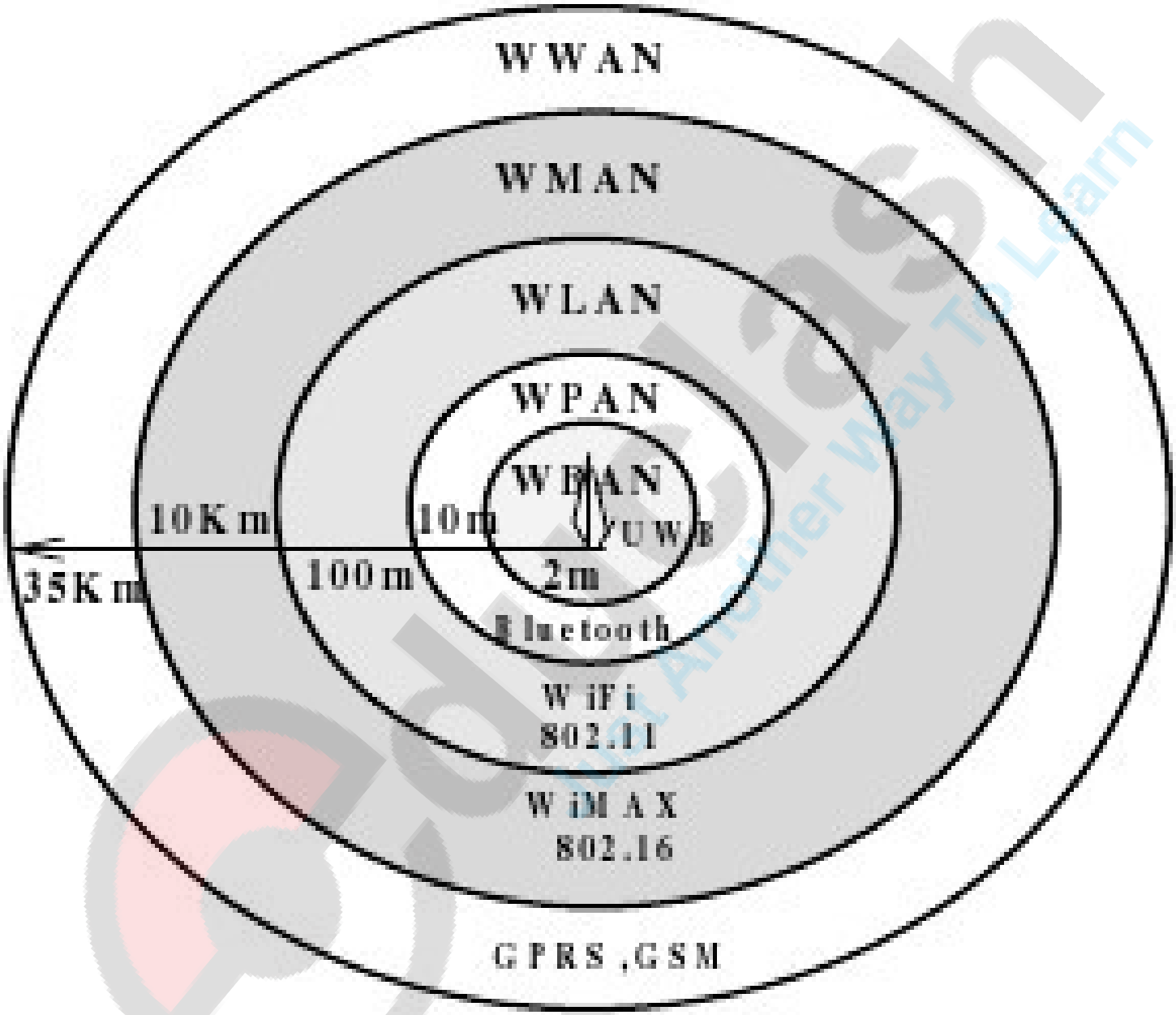
- Mobile hosts
- Fixed hosts
- Access networks consisting of access stations
- Core network(mobility and switching)

- **Mobile hosts:**
  - Mobile phone, laptop etc.
  - Can move from one access area to another.
- **Fixed wireless host:**
  - Immobile.
  - e.g. wireless web servers, printers etc.
- **Access network:**
  - Accesss stations covering a certain geographical area.
  - Base station/ access point/ wireless router.
- **Core Network:**
  - Active components to perform data switching.
  - Provide location and mobility services.

Classification of wireless networks

Based on geographical coverage and infrastructure:

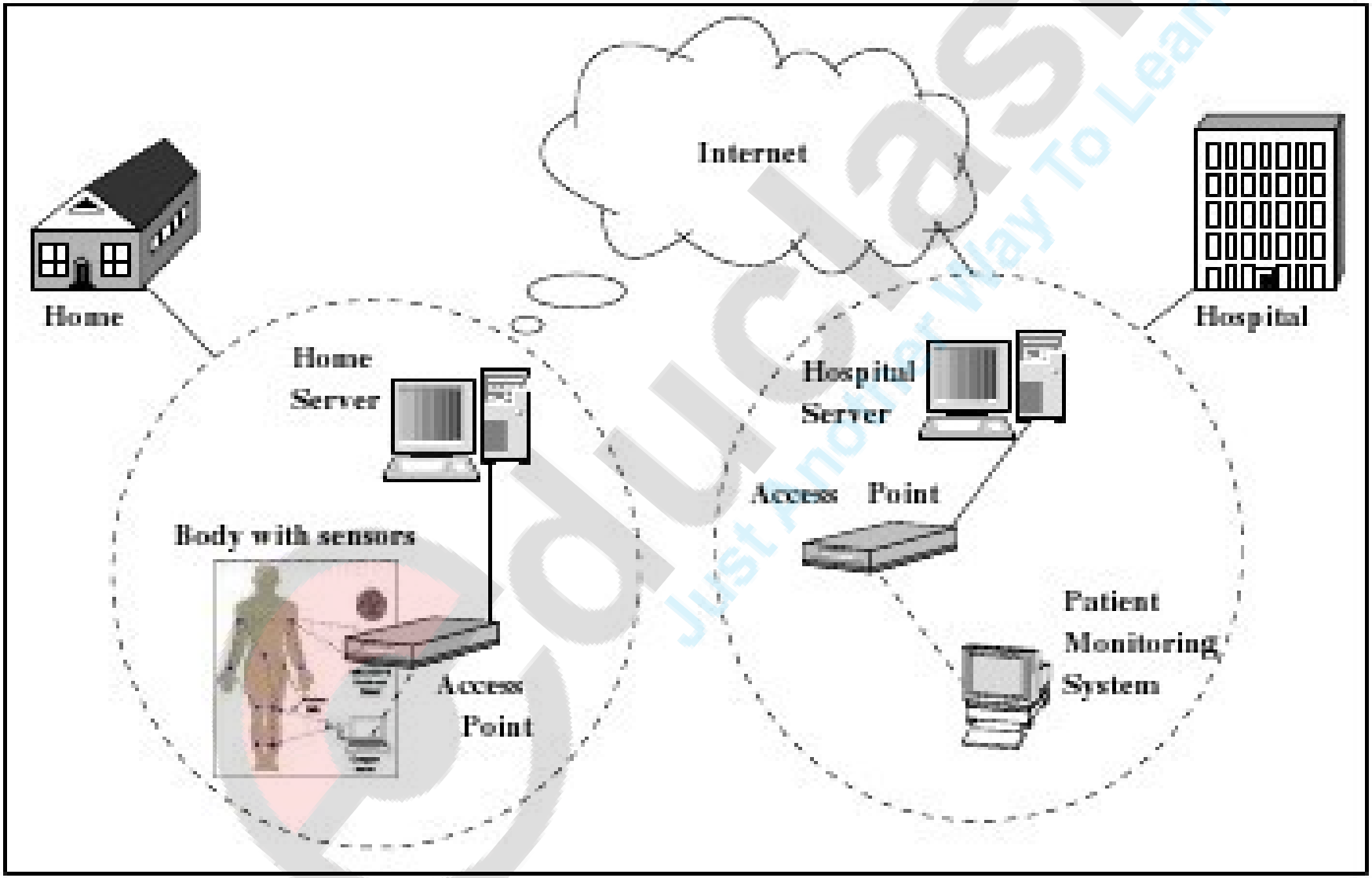
- Wireless body area networks (WBANs)
- Wireless personal area networks (WPANs)
- Wireless local area networks (WLANs)
- Wireless metropolitan area networks (WMANs)
- Wireless wide area networks (WWANs)
- Satellite networks
- Broadband access networks


WWAN
WMAN
WLAN
WPAN
WBAN
UWB
10Km
10m
35Km
100m
2m
Bluetooth
WiFi
802.11
WiMAX
802.16
GPRS ,GSM

Wireless body area networks (WBANs)

- Maximum signal range of 2 m.
- Used for interconnecting respective devices to one another within the surface of the body.
- Set of mobile and compact intercommunicating sensors (wearable/implanted) into human body.
- Technical requirements:
  - Frequency range below 6GHz.
- Applications:
  - Health industry, sports, military, security.

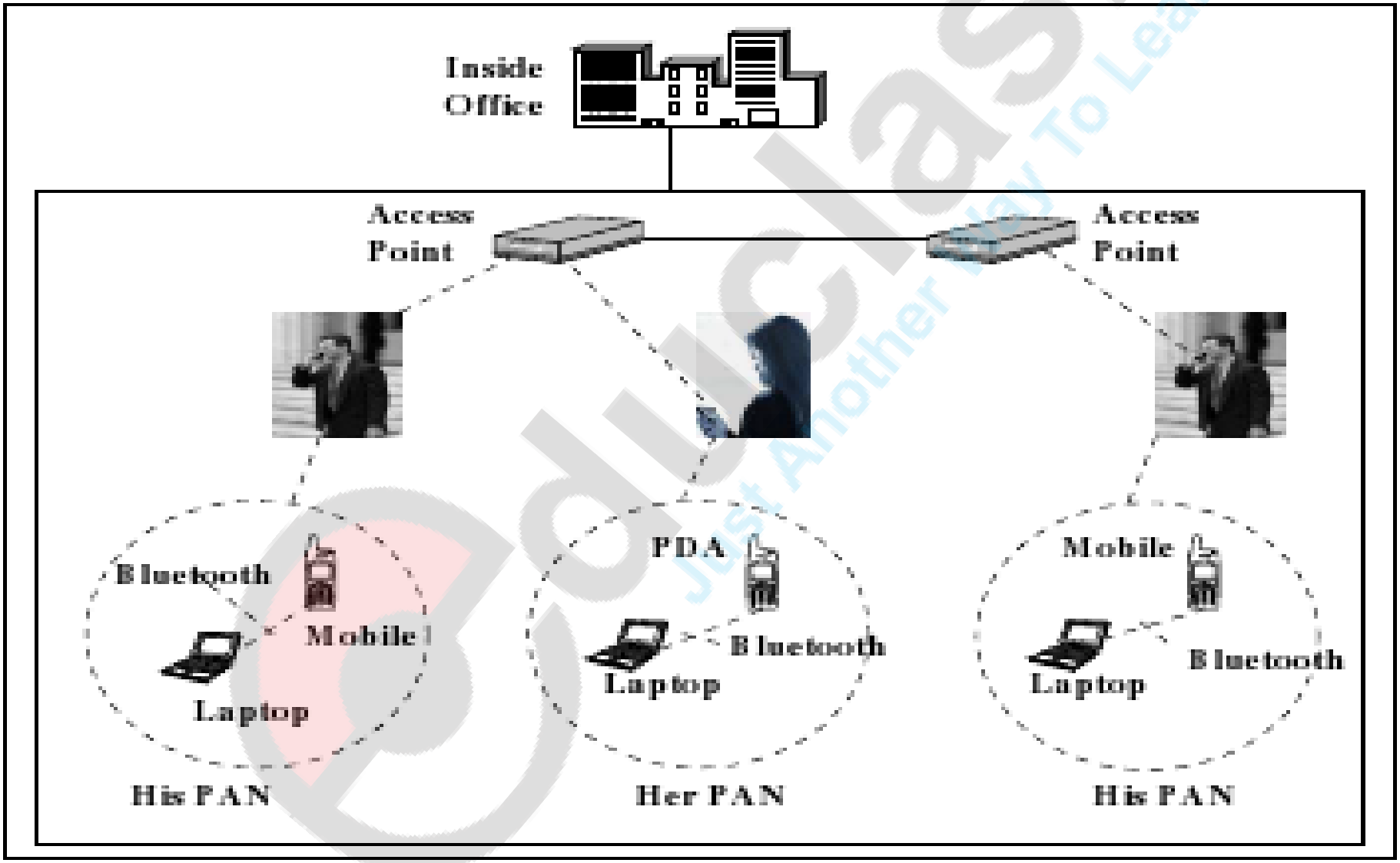
WBAN application scenario



Wireless personal area networks (WPANs)

- Maximum signal range of 10 m.
- Used for interconnecting respective devices to one another. (e.g. telephones).
- Used for communication among personal devices/ connecting higher level network and internet.
- e.g. Bluetooth.

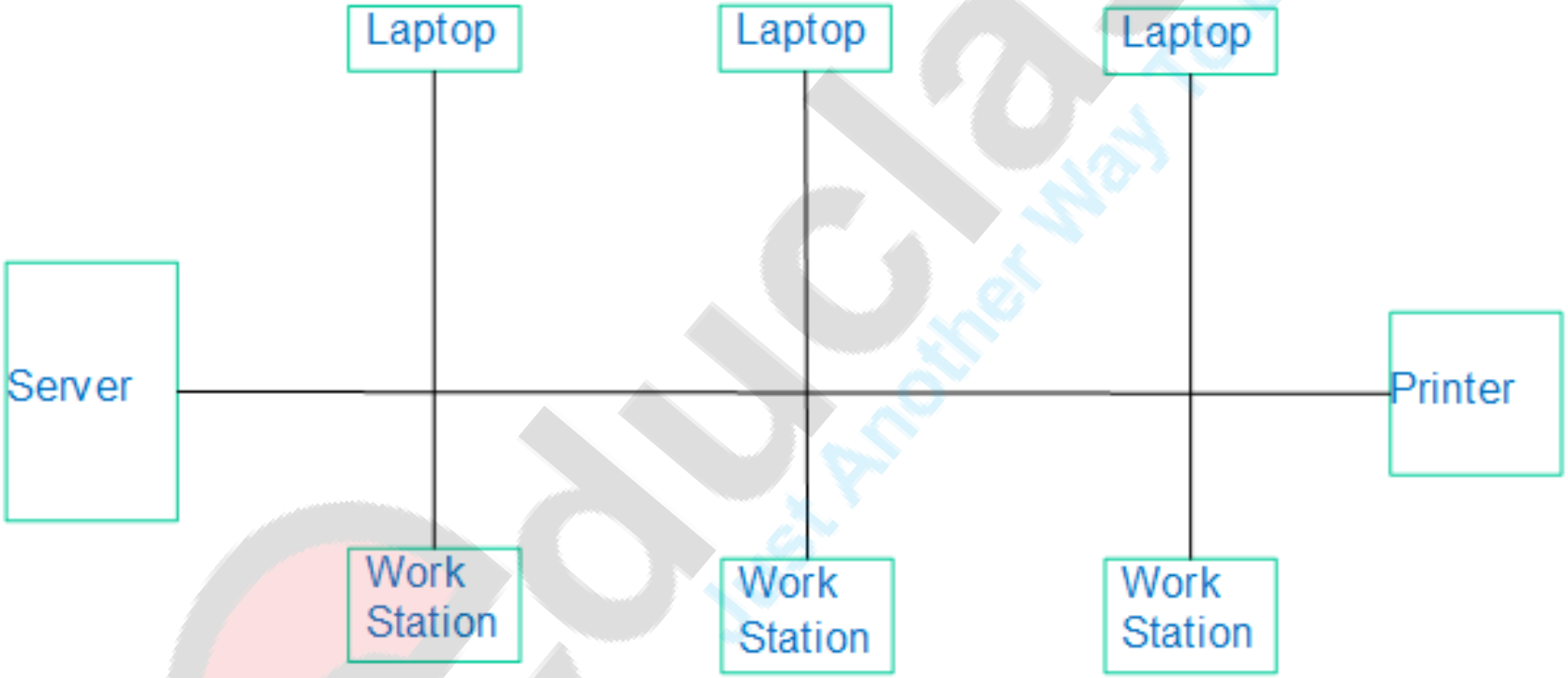
WPAN application scenario



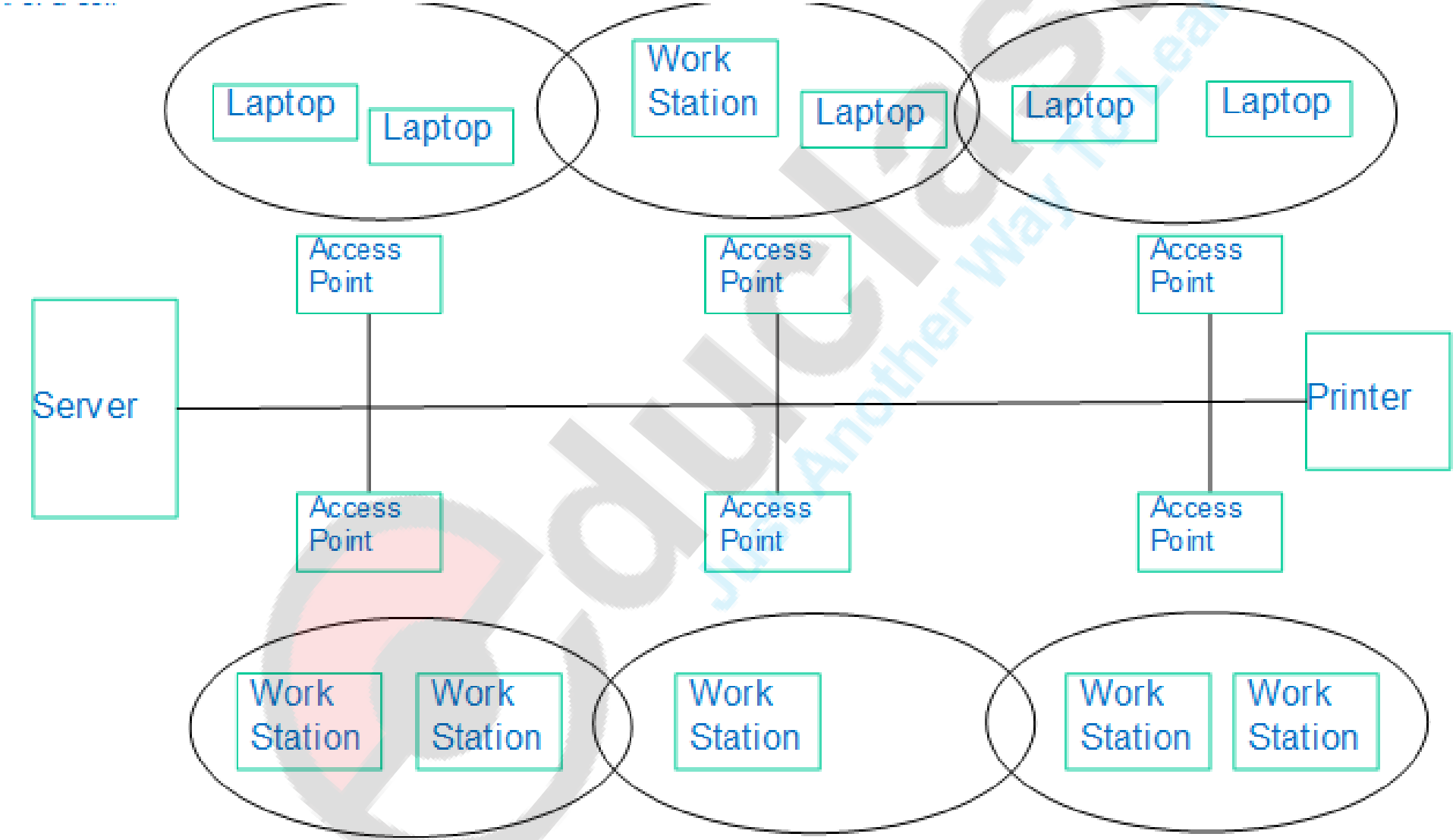
Wireless local area networks (WLANs)

- Signal range - approx. 30 m indoors and 100-200 m outdoors.
- For the range of one room or one building.
- Linking a group of computers in a small campus.
- Uses spread spectrum or OFDM.
- Wi-Fi- most common used technology of WLANs.

Wired LAN


Laptop
Laptop
Laptop
Server
Printer
Work Station
Work Station
Work Station

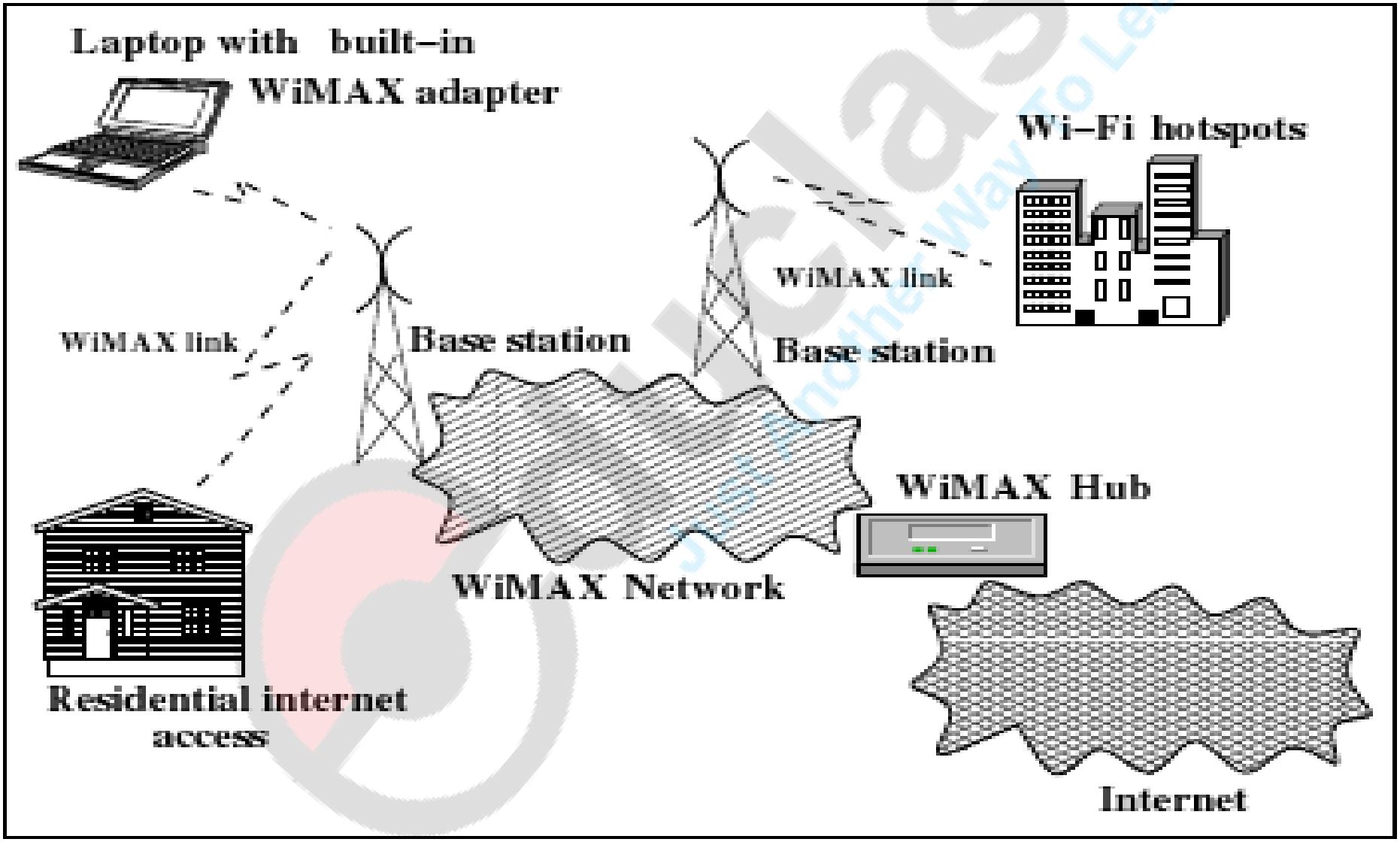
Wireless LAN



Wireless metropolitan area networks (WMANs)

- Signal range of approx. 5-20 km but can span up to 50 km.
- Used to connect user to internet- broadband internet access from fixed or mobile devices.
- Provides inter-networking of local networks.
- Often called worldwide interoperability for microwave access (WiMAX or IEEE 802.16).
- Can be owned by a single oraganization or group of organizations.

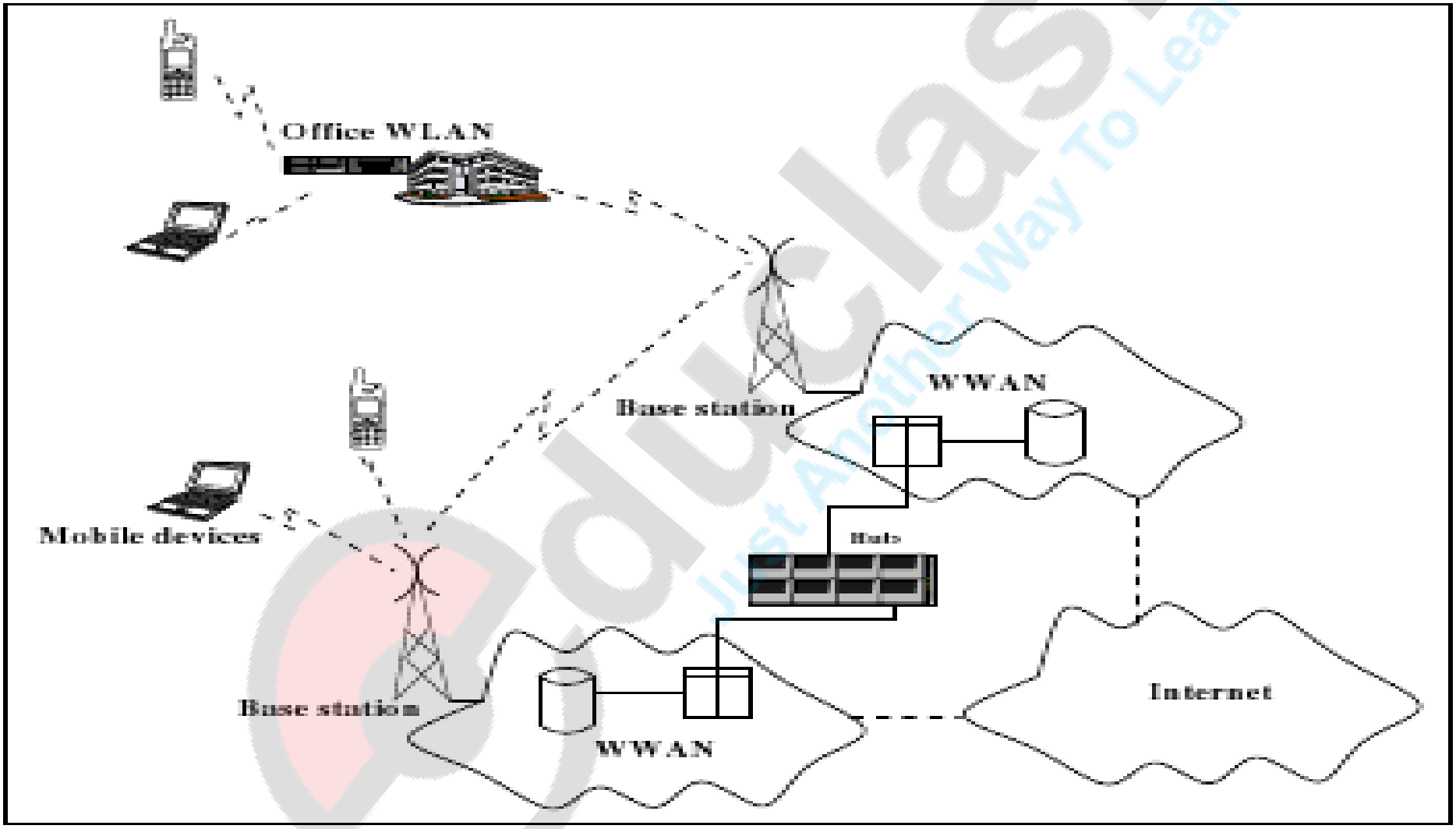
WMAN


Laptop with built–in
WiMAX adapter
Wi–Fi hotspots
WiMAX link
WiMAX link
Base station
Base station
WiMAX Hub
WiMAX Network
Residential internet
access
Internet

Wireless wide area networks (WWANs)

- GSM and CDMA based networks.
- Employs network infrastructure of mobile operators.
- Covers a broad geographical area.
- e. g. internet.
- Used to connect WLANs together.
- Requires wireless modems and a wireless network infrastructure.
- Services are offered regionally, nationwide or globally by wireless service providers for a monthly usage fee.

WWAN


Office WLAN
Base station
WWAN
Mobile devices
Hub
Base station
WWAN
Internet

IEEE 802.11

Advantages of WLAN:

- Flexibility
- Planning
- Design
- Robustness
- Cost

Disadvantages of WLAN:

- Quality of service
- Proprietary solutions
- Restrictions
- Safety and security

Technologies used to set up WLAN

Infrared transmission:

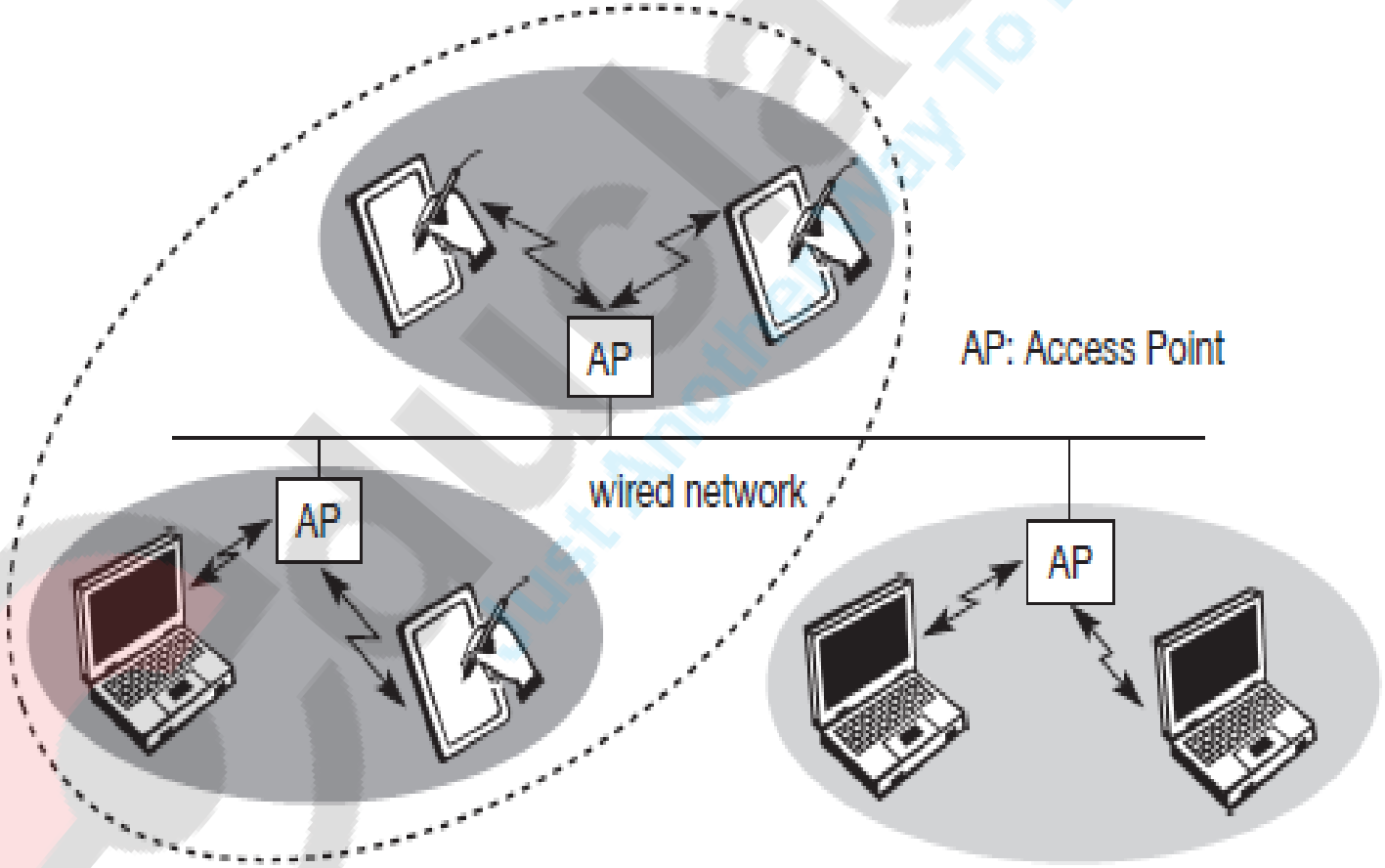
- 900 nm wavelength.
- Uses diffuse light or directed light.
- Senders- LEDs or Laser diodes.
- Receivers- photodiodes.
- Advantage-Simple and cheap.
- Disadvantage-Low bandwidth.

Radio transmission:

- 2.4 GHz.
- Advantage-Cover larger areas.
- Disadvantage- interference with other signals.

Infrastructure based wireless network

Figure 7.1
Example of three infrastructure-based wireless networks



Ad-hoc wireless networks

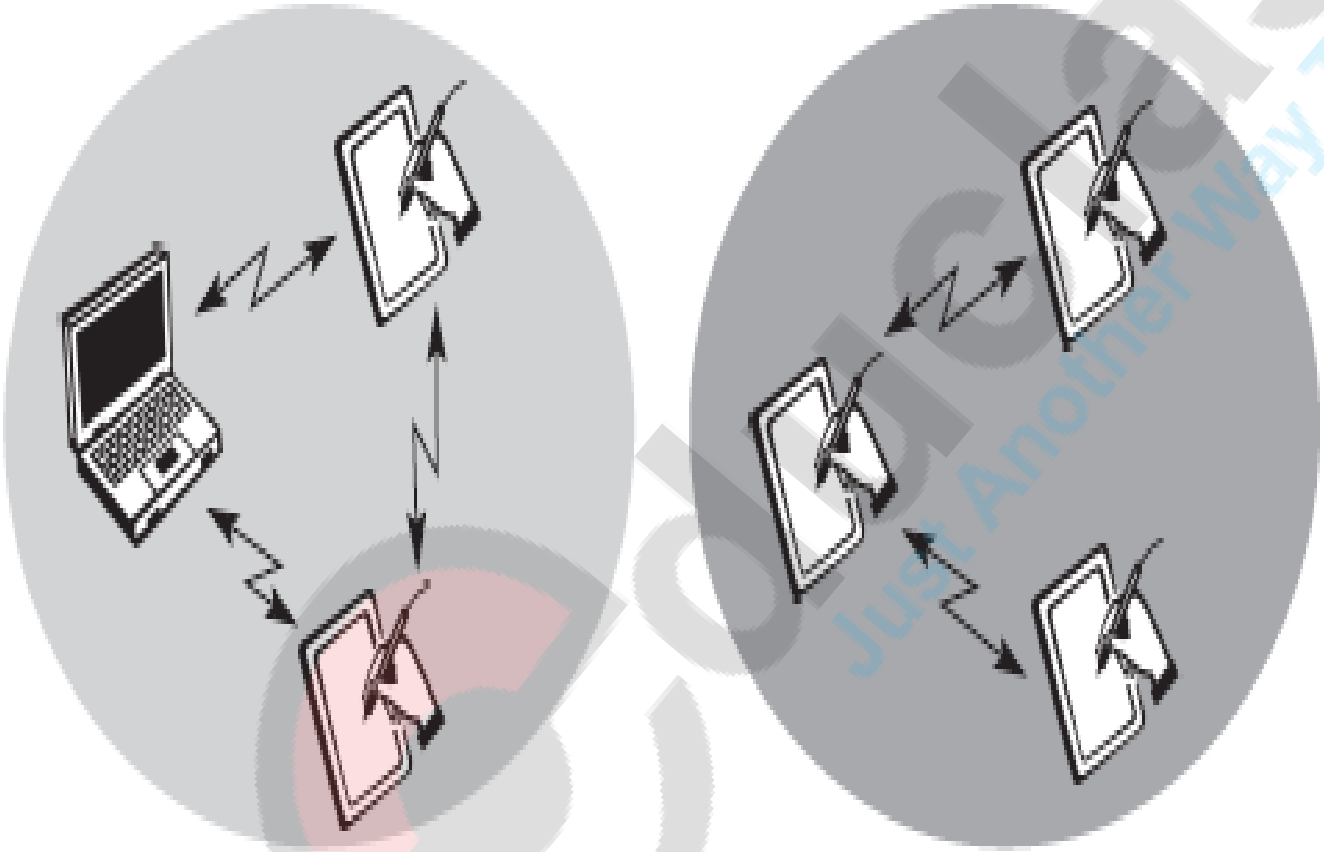


Figure 7.2
Example of two ad-hoc wireless networks

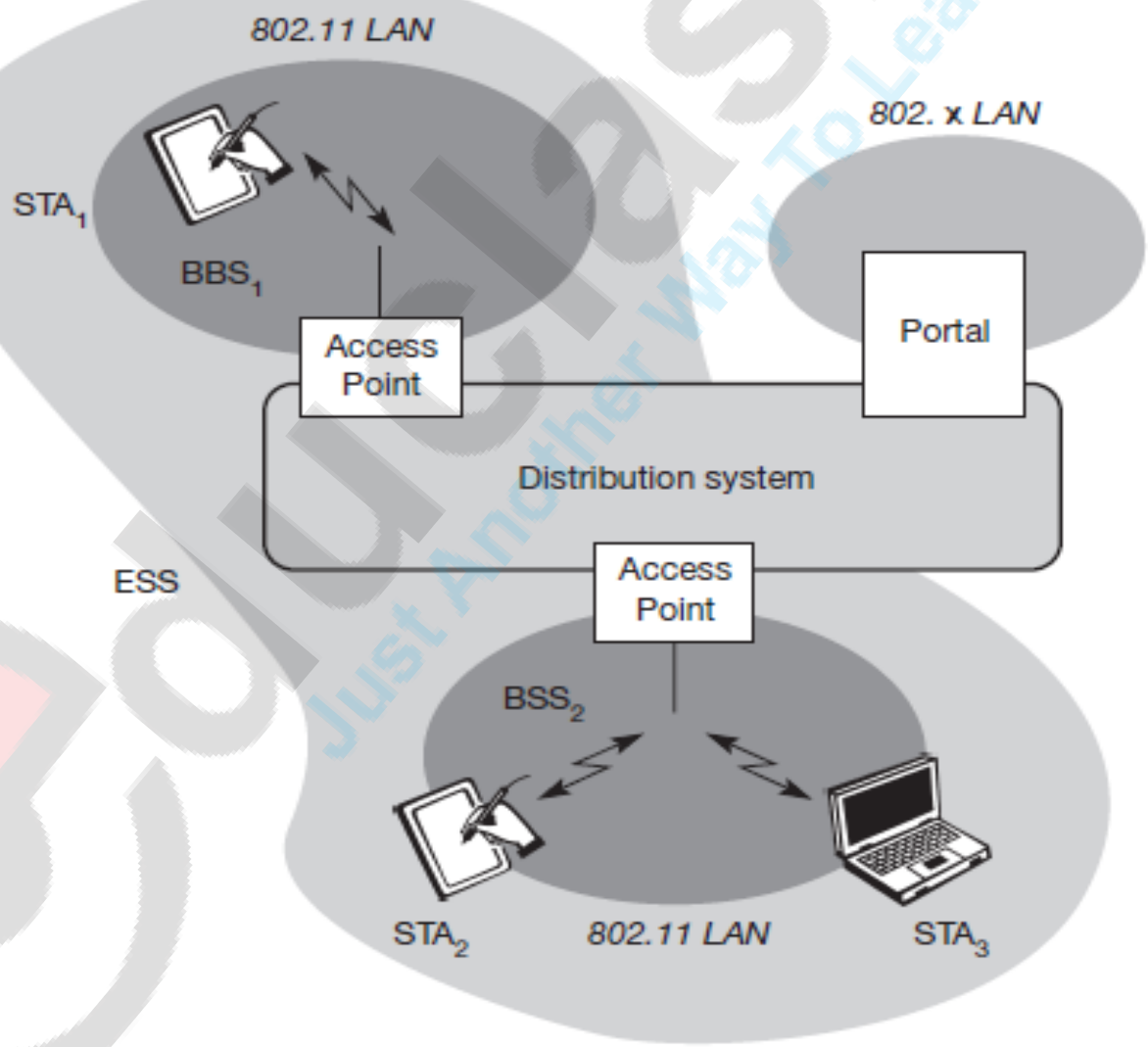
WLAN- IEEE 802.11

Characteristics of IEEE 802.11

- Famous family of WLANs.
- Simple and robust.
- Offers time bounded and asynchronous services.
- Physical layer- infrared and spread spectrum radio transmission.
- Power management.
- 2.4 GHz ISM band.

Architecture of Infrastructure based IEEE 802.11

Figure 7.3
Architecture of an infrastructure-based IEEE 802.11



- STA- stations.
- AP- access points.
- BSS- Basic service set.
- ESS- Extended service set.
- ESSID.
- IBSS- independent BSS.

Architecture of IEEE 802.11 ad-hoc wireless LANs

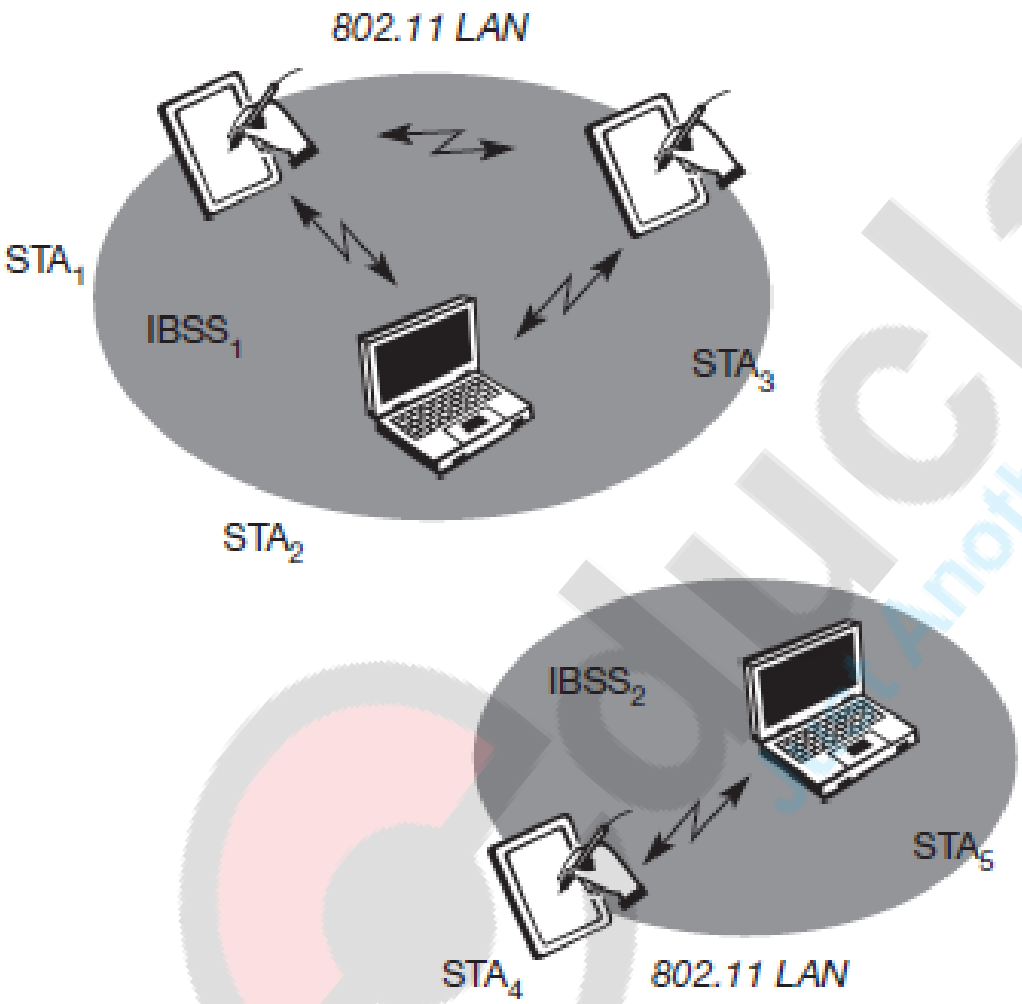
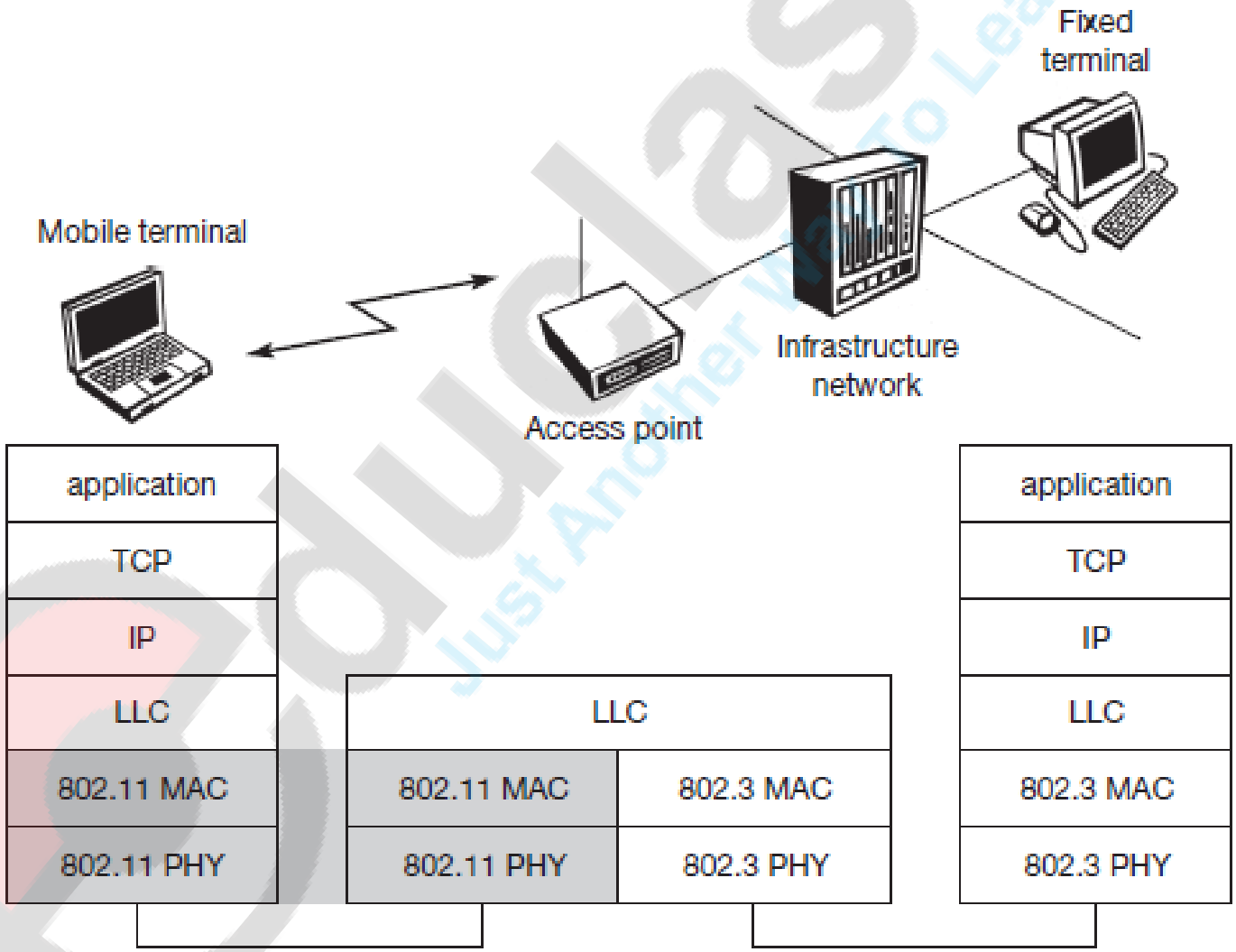


Figure 7.4
Architecture of IEEE 802.11 ad-hoc wireless LANs

Protocol architecture

Figure 7.5
IEEE 802.11
protocol architecture
and bridging



- PLCP- Physical layer convergence protocol.
  - Provides carrier sense signal(Clear channel assignment-CCA)
  - Provides Service access points(SAP)
- PMD- physical medium dependent.
  - Modulation and encoding/decoding of signals.
- MAC layer
  - Medium access
  - Fragmentation of user data
  - Encryption

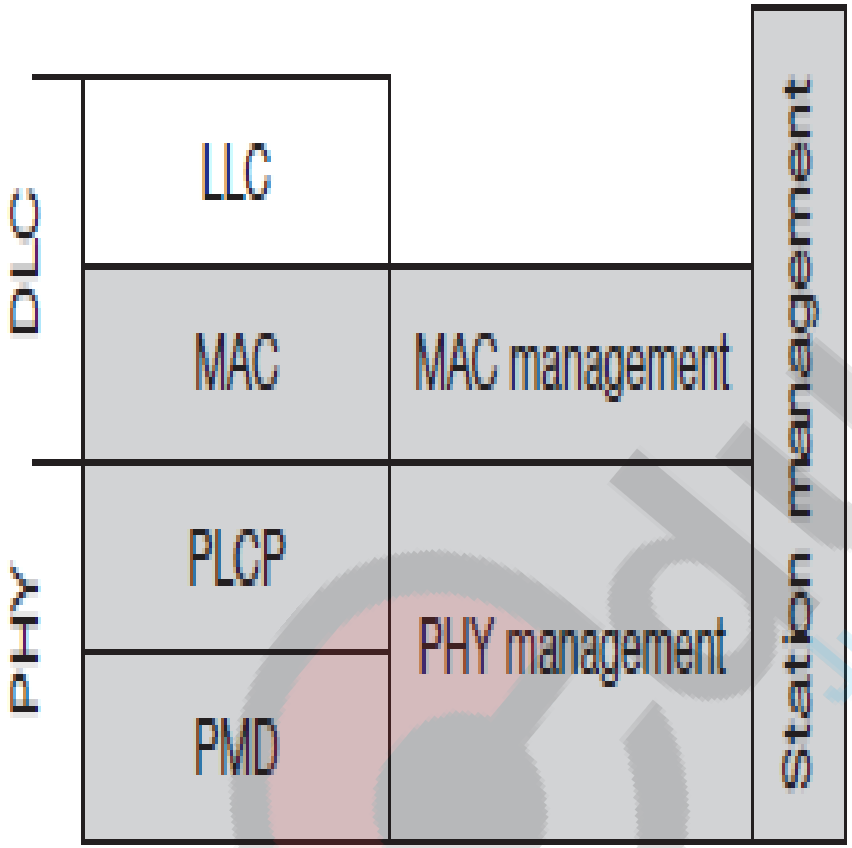


Figure 7.6
Detailed IEEE 802.11 protocol architecture and management

- MAC management:
  - Association and re-association of stations to Access points.
  - Roaming between different AP
  - Authentication, encryption, synchronization.
  - Power management.
  - Maintains MIB- Management information base.
- PHY management:
  - Channel tuning and PHY MIB maintenance.
- Station management:
  - Interaction with both management layers.
  - Control of bridging and interaction with distribution system.

Physical layer

3 versions: 2 radio (typ. 2.4 GHz), 1 IR

- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying),
- DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared

- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

802.11 - MAC layer I – DFWMAC (Distributed foundation wireless MAC)

Traffic services

- Asynchronous Data Service (mandatory)
- exchange of data packets based on “best-effort”

Time-Bounded Service (optional)

- implemented using PCF (Point Coordination Function)

Access methods

- DFWMAC-DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DFWMAC-DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - avoids hidden terminal problem

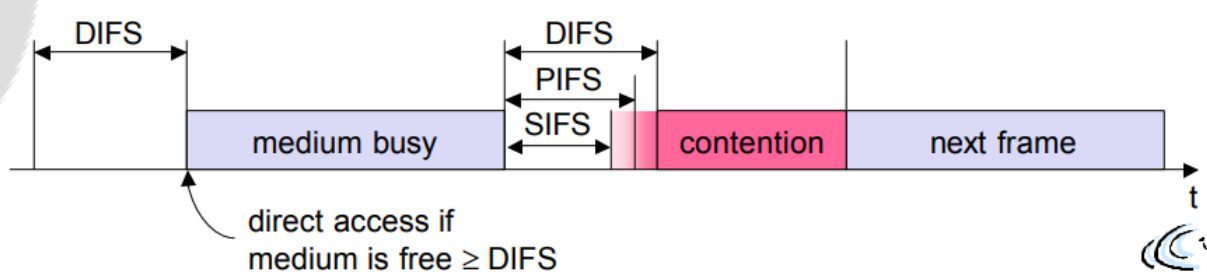
- DFWMAC- PCF (optional)
  - access point polls terminals according to a list

Priorities

- defined through different inter frame spaces
- no guaranteed, hard priorities
- For controlling waiting time

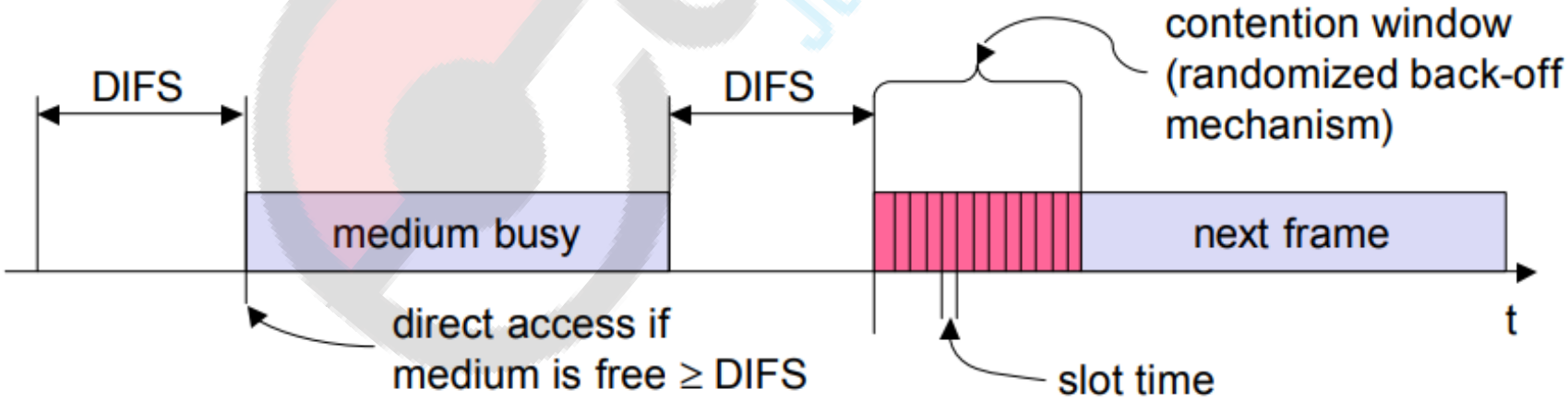
Slot time- by propogation delay , transmitter delay etc. 50 μs for FHSS and 20 μs for DSSS

- SIFS (Short Inter Frame Spacing) :
  - highest priority, for ACK, CTS, polling response.
  - For DSSS SIFS is 10 μs and for FHSS it is 28 μs.
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF.
  - SIFS plus one time slot.
- DIFS (DCF, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service.
  - SIFS plus two time slots



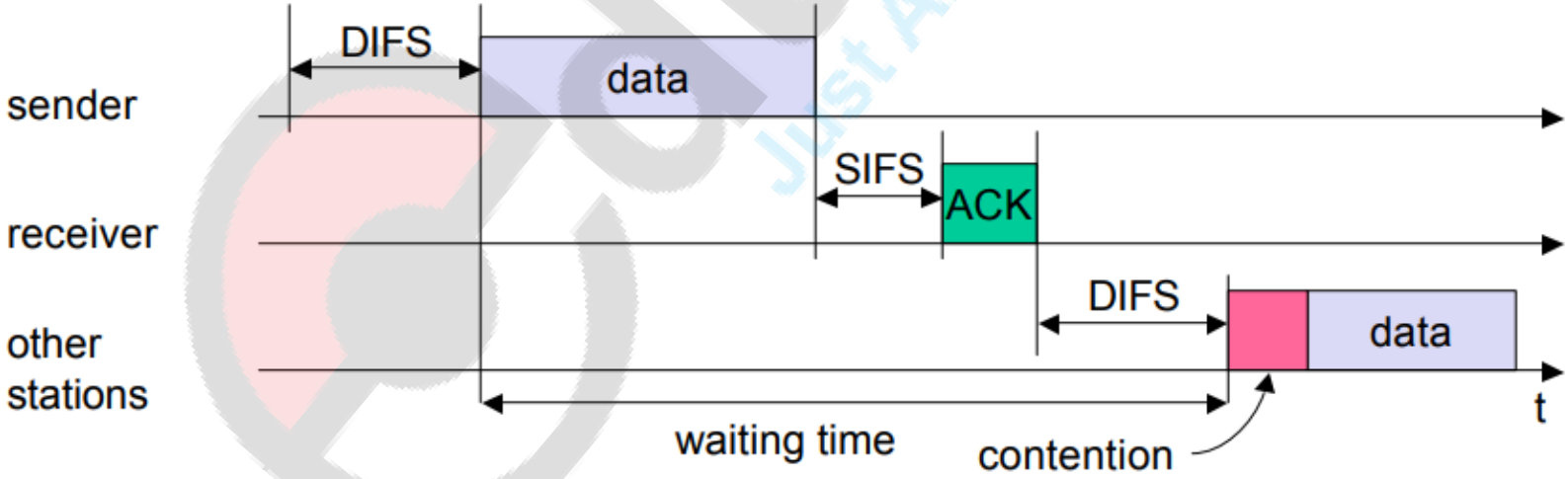
802.11 - CSMA/CA access method I

- station ready to send senses medium (based on PHY layer CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
- If multiple stations have backed off, when 1 timer expires, other timers frozen

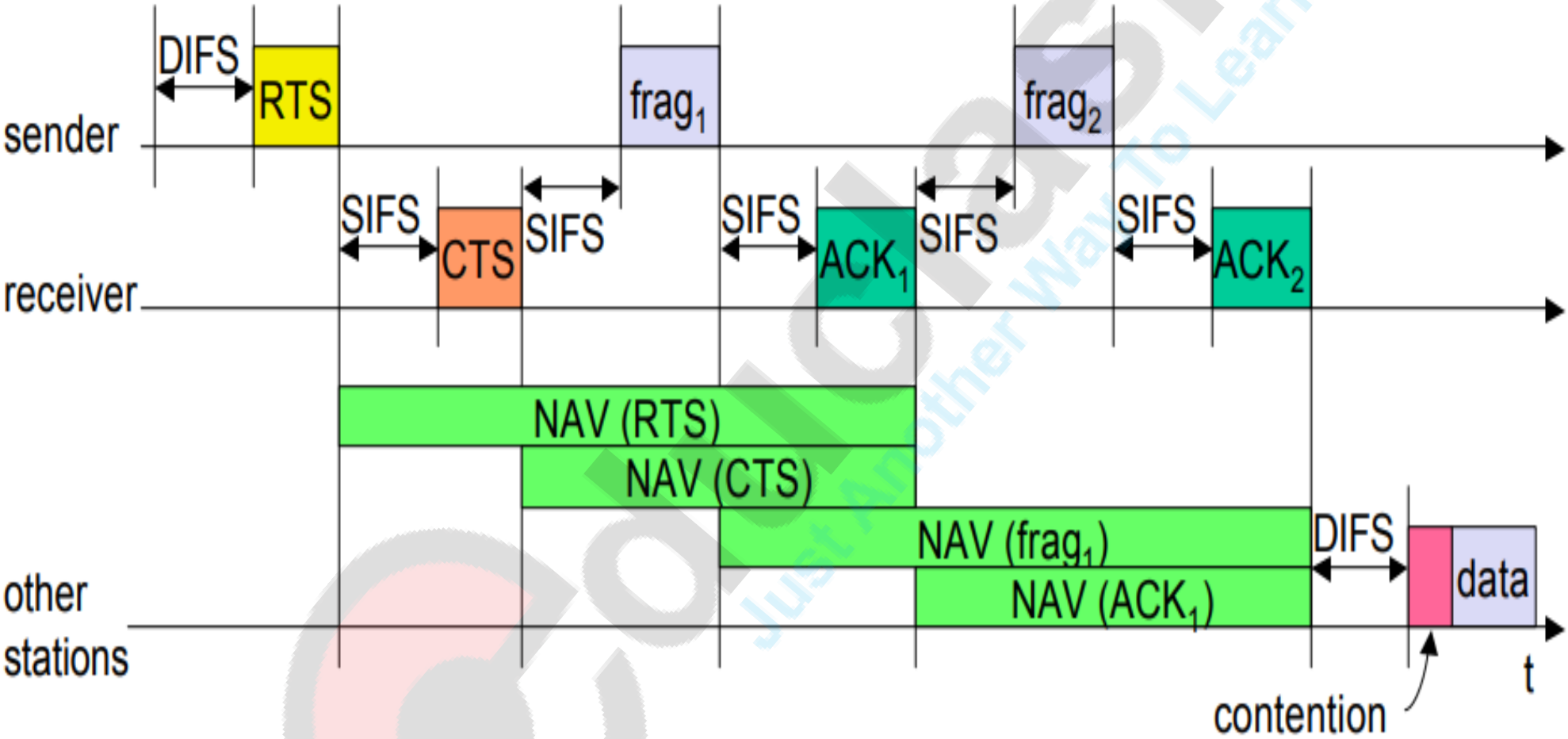


802.11 - CSMA/CA access method II

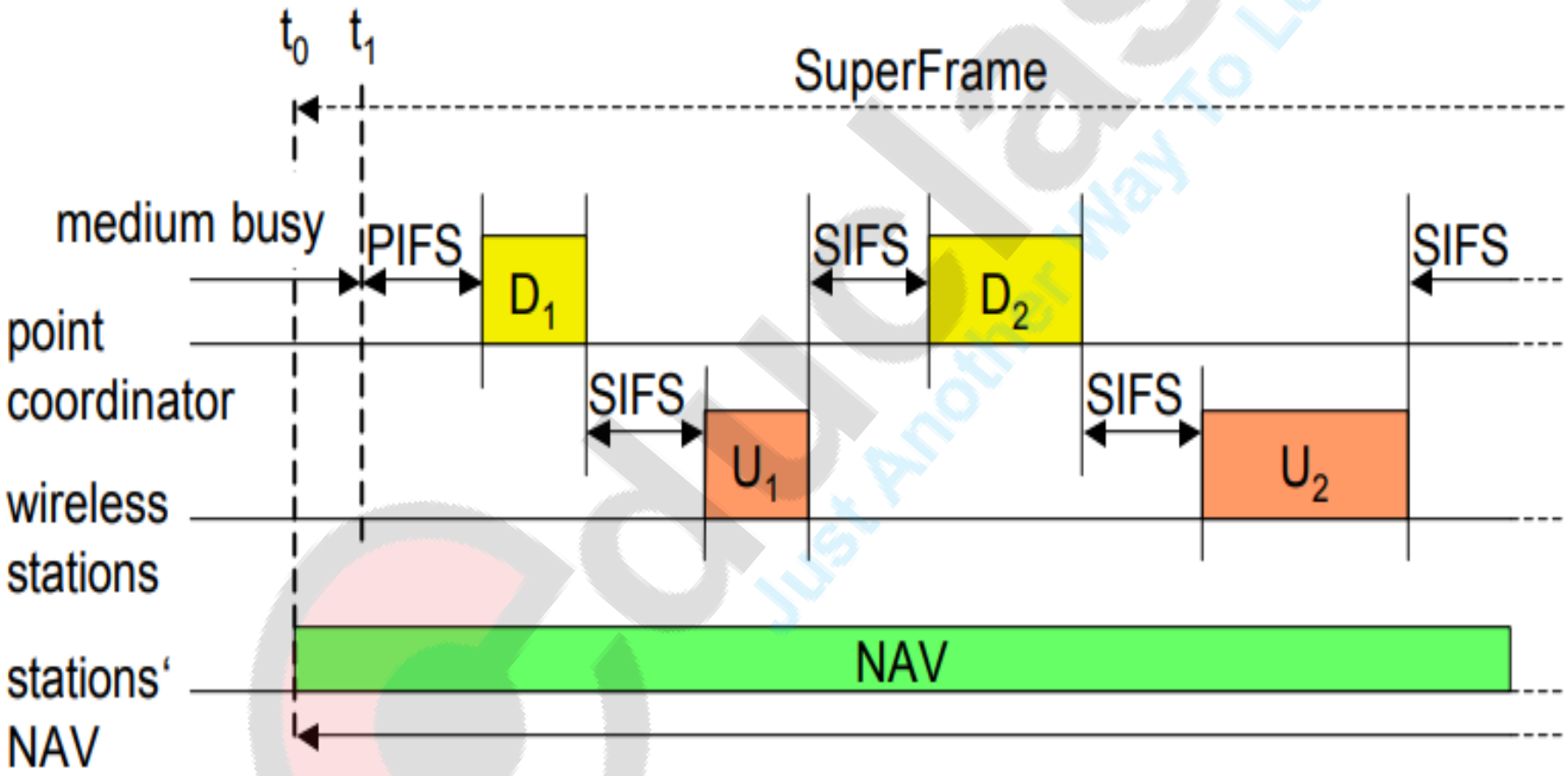
- Sending unicast packets
- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



Fragmentation

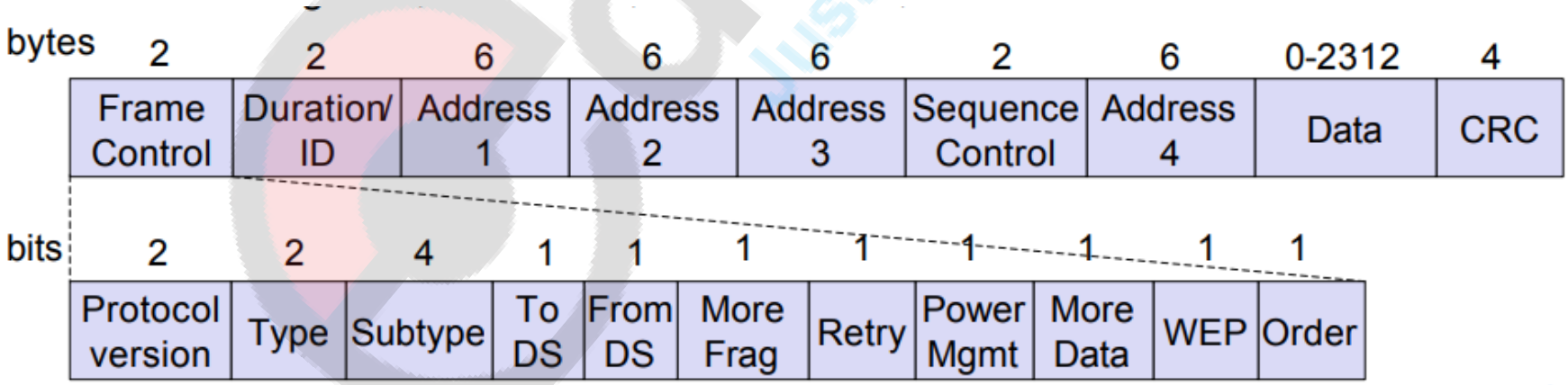


DFWMAC-PCF I


t_0
t_1
SuperFrame
medium busy
PIFS
D_1
SIFS
D_2
SIFS
point coordinator
SIFS
U_1
SIFS
U_2
wireless stations
NAV
stations' NAV

802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKS
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data



802.11 - MAC management

Synchronization

- Clock skew may happen
- Infrastructure: AP broadcasts beacons, other nodes correct skew
- Ad hoc: All nodes broadcast beacons

Power management

- Save battery, nodes can go to sleep, wake up periodically to receive
- Infrastructure: AP buffers packets for sleeping nodes
- Ad hoc: sender buffers packets for sleeping destinations

Association/Reassociation

- Roaming: Move from access point to access point as user moves
- scanning, i.e. active search for a network
- Node sends message to new AP, says goodbye to old AP

MIB - Management Information Base

- All information for managing network, node stored in SNMP MIB
- MIB can be read (access) or written to (update)

WLAN: IEEE 802.11a

Data rate

- 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
- User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
- 6, 12, 24 Mbit/s mandatory

Transmission range

- 100m outdoor, 10m indoor
  - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m

Frequency

- Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

Security

- Limited, WEP insecure, SSID

Availability

- Some products, some vendors

Connection set-up time

- Connectionless/always on

Quality of Service

- Typ. best effort, no guarantees (same as all 802.11 products)

Manageability

- Limited (no automated key distribution, sym. Encryption)

Special Advantages/Disadvantages

- Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
- Disadvantage: stronger shading due to higher frequency, no QoS

WLAN: IEEE 802.11b

Data rate

- 1, 2, 5.5, 11 Mbit/s, depending on SNR
- User data rate max. approx. 6 Mbit/s

Transmission range

- 300m outdoor, 30m indoor
- Max. data rate ~10m indoor

Frequency

- Free 2.4 GHz ISM-band

Security

- Limited, WEP insecure, SSID

Availability

- Many products, many vendors

Connection set-up time

- Connectionless/always on

Quality of Service

- Typ. Best effort, no guarantees (unless polling is used, limited support in products)

Manageability

- Limited (no automated key distribution, sym. Encryption)

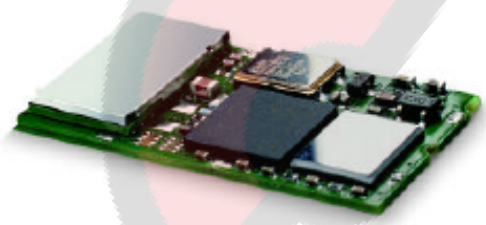
Special Advantages/Disadvantages

- Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
- Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

Bluetooth- IEEE 802.15

Bluetooth- IEEE 802.15

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell
- Phones.
- Embedded in other devices
- Short range (10 m), low power consumption, license-free 2.45 GHz.
- Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first modules (Ericsson).

Characteristics

2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing

- Channel 0: 2402 MHz … channel 78: 2480 MH
- G-FSK modulation, 1-100 mW transmit power

FHSS and TDD

- Frequency hopping with 1600 hops/s
- Hopping sequence in a pseudo random fashion, determined by a master
- Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)

- FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)

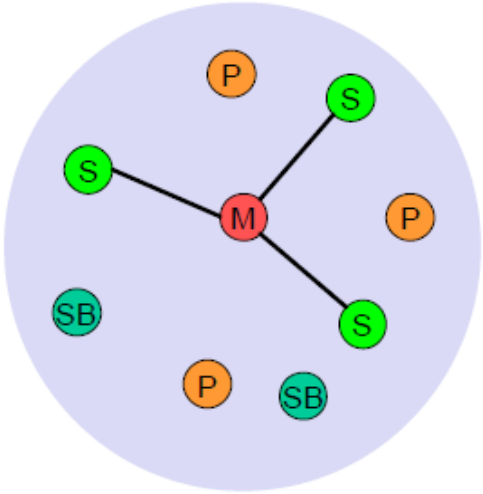
- Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s
- symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

Topology

- Overlapping piconets (stars) forming a scatternet

Piconet

- Collection of devices connected in an ad-hoc fashion.
- One unit acts as master and the others as slaves for the lifetime of the piconet.
- Master determines hopping pattern, slaves have to synchronize.
- Each piconet has a unique hopping pattern.
- Participation in a piconet = synchronization to hopping sequence.
- Each piconet has one master and up to 7 slaves.
- simultaneous slaves (> 200 could be parked).



M=Master
S=Slave
P=Parked
SB=Standby

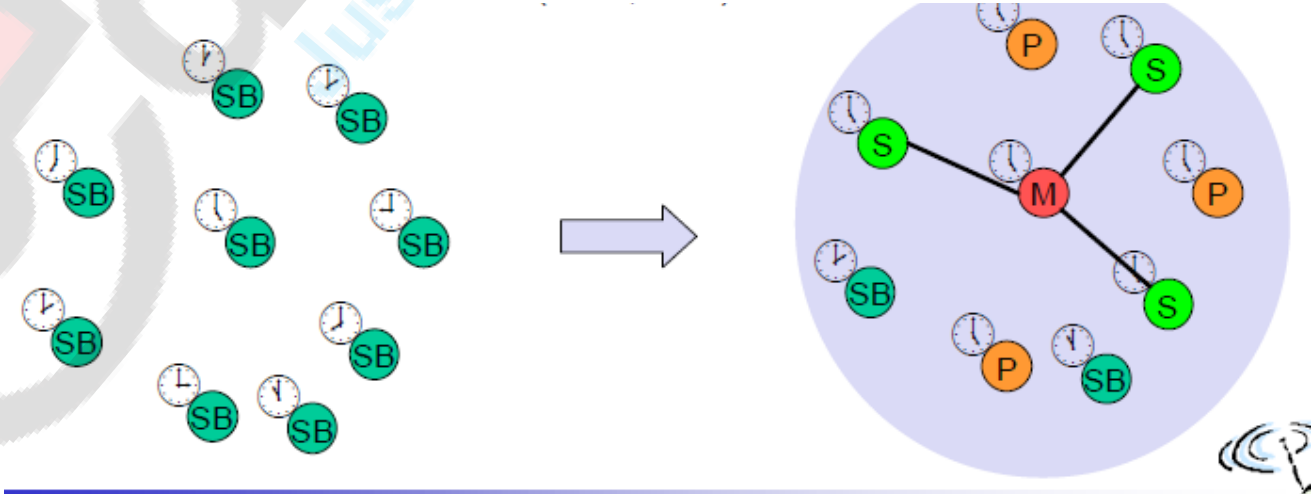
Forming a piconet

All devices in a piconet hop together

- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock

Addressing

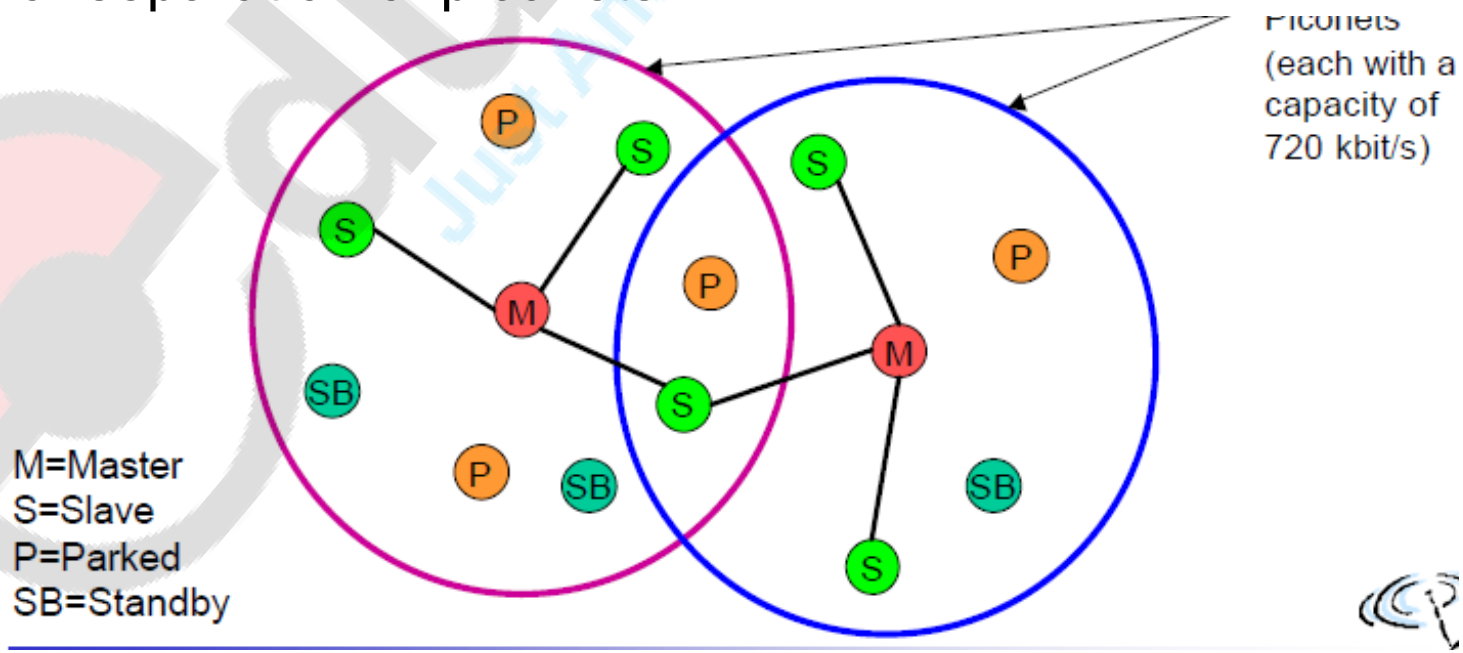
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



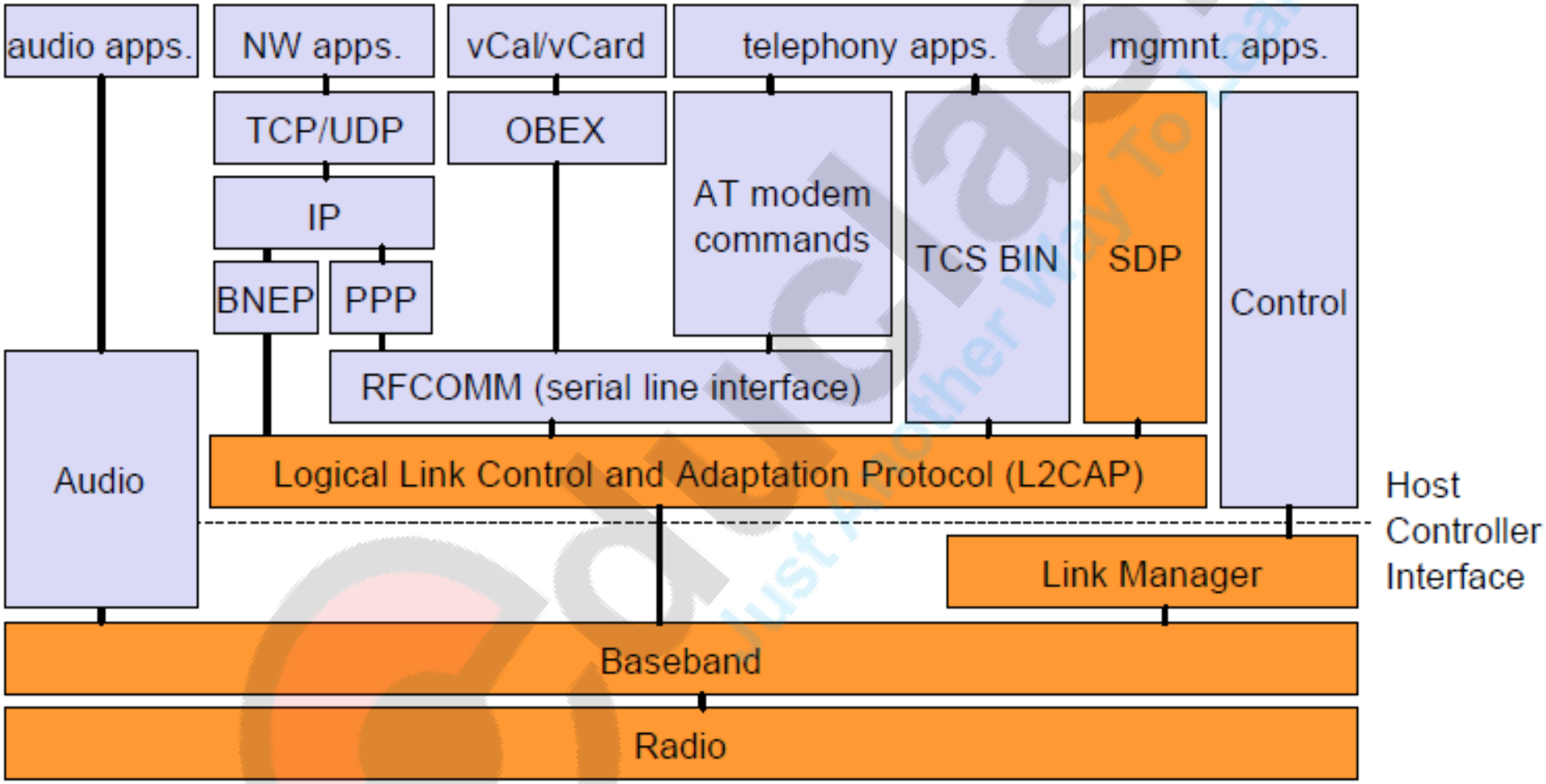
Scatternet

- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another.
- Communication between piconets
  - Devices jumping back and forth between the piconets.

FH-CDMA is used for separation of piconets.



Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

Core Protocols:

Radio:
Specification of the air interface, i.e., frequencies, modulation, and transmit power.

Baseband:
Description of basic connection establishment, packet formats, timing, and basic QoS parameters.

Link manager protocol:
Link set-up and management between devices including security functions.

Logical link control and adaptation protocol (L2CAP):
Adaptation of higher layers to the baseband - connectionless and connection-oriented services.

Service discovery protocol:
Device discovery in close proximity and querying of service characteristic.

- **cable replacement protocol RFCOMM**
  - replacement of serial line cables
  - enables many legacy applications and protocols to run over Bluetooth.

- **telephony control protocol specification – binary (TCS BIN):**
  - call control signalling for the establishment of voice and data calls between Bluetooth devices.
  - describes mobility and group management functions.

- **host controller interface (HCI)**
  - between the baseband and L2CAP provides a command interface to the baseband controller and link manager.
  - access to the hardware status and control registers.
  - hardware/software boundary.

- Many protocols have been **adopted** in the Bluetooth standard.

- Classical Internet applications can still use the standard TCP/IP stack running over PPP or use the more efficient **Bluetooth network encapsulation protocol (BNEP).**

- Telephony applications can use the AT modem commands as if they were using a standard modem.

- Calendar and business card objects (**vCalendar/vCard**) can be exchanged using the object exchange protocol (**OBEX**) as common with IrDA interfaces.

- Audio applications may directly use the baseband layer after encoding the audio signals.

Radio layer

- defines the carrier frequencies and output power.
- Bluetooth uses the license-free frequency band at 2.4 GHz allowing for worldwide operation with some minor adaptations to national restrictions.
- A frequency-hopping/time-division duplex scheme is used for transmission, with a fast hopping rate of 1,600 hops per second.
- The time between two hops is called a slot, which is an interval of 625 μs.
- Each slot uses a different frequency.
- Bluetooth uses 79 hop carriers equally spaced with 1 MHz.

Bluetooth transceivers use Gaussian FSK for modulation.

Power class 1:

Maximum power is 100 mW and minimum is 1 mW (typ. 100 m range without obstacles). Power control is mandatory.

Power class 2:

Maximum power is 2.5 mW, nominal power is 1 mW, and minimum power is 0.25 mW (typ. 10 m range without obstacles). Power control is optional.

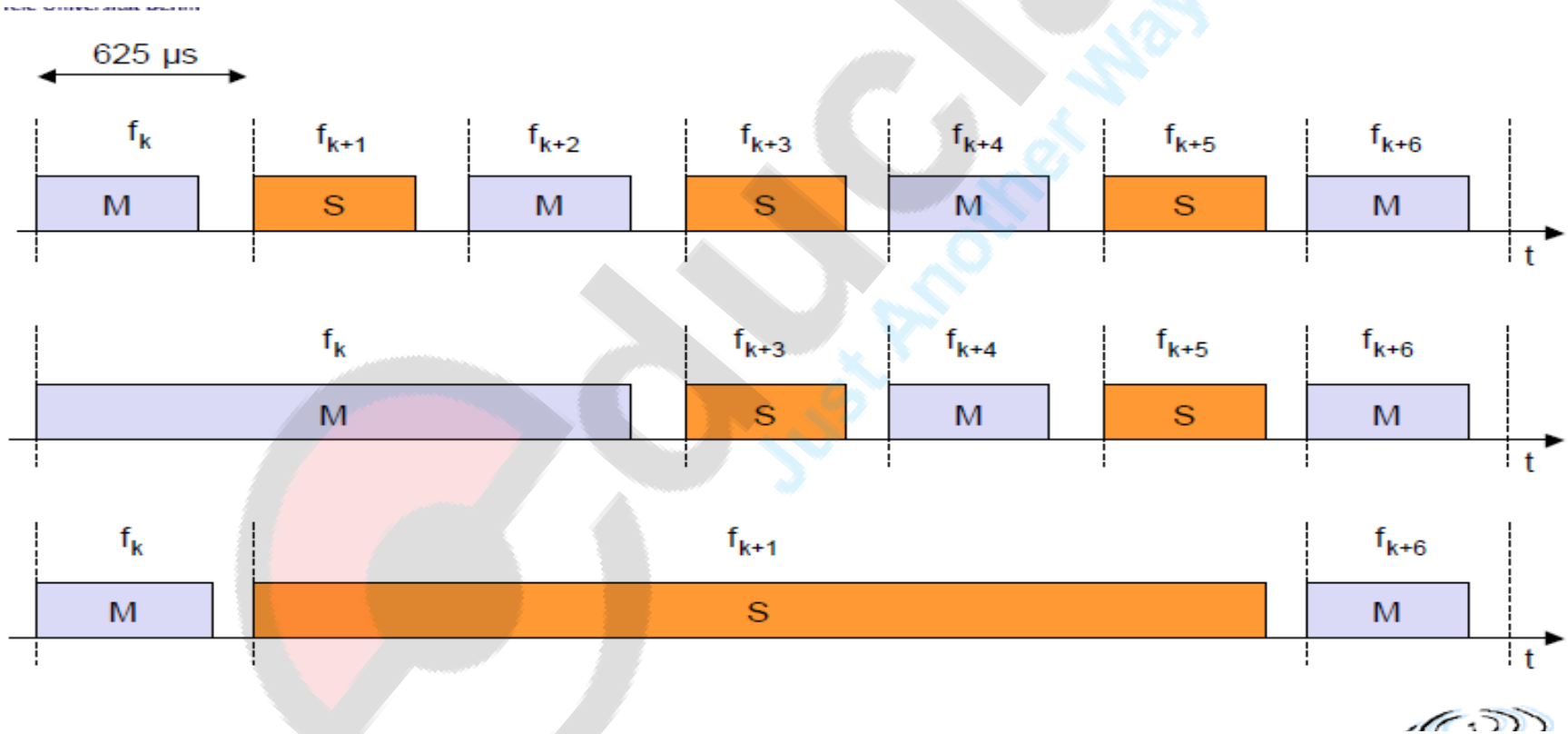
Power class 3:

Maximum power is 1 mW.

Baseband layer

- performs frequency hopping for interference mitigation and medium access.
- but also defines physical links and many packet formats.

- **Frequency selection during data transmission**



Baseband link types

- Polling-based TDD packet transmission

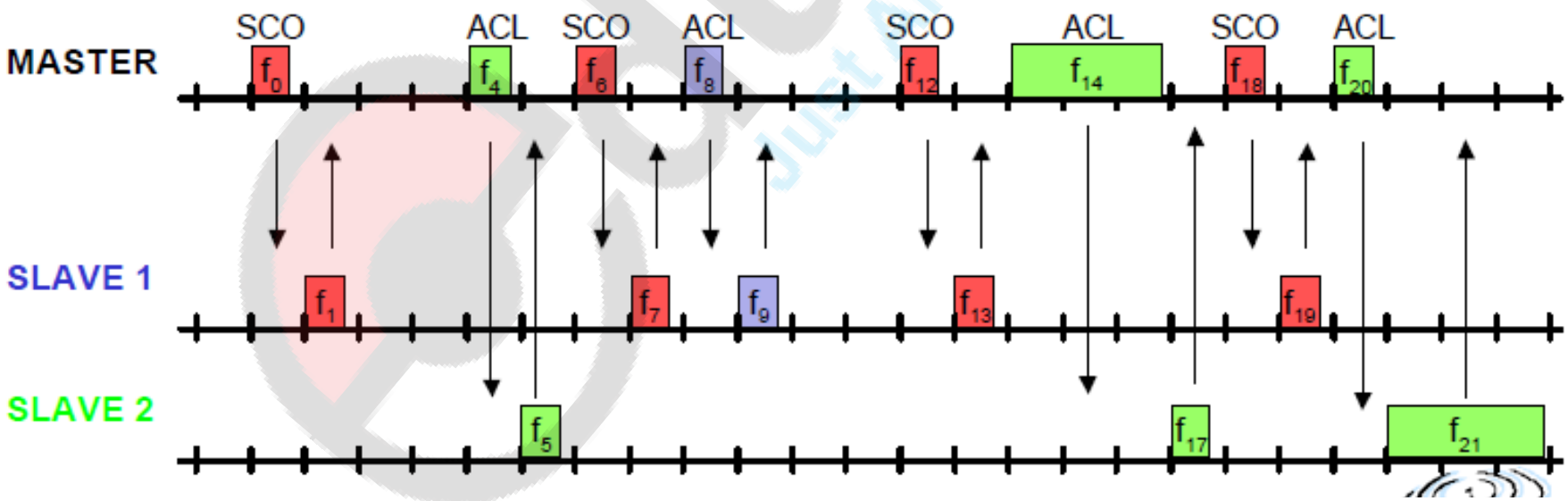
  625µs slots, master polls slaves.

- SCO (Synchronous Connection Oriented) – Voice

  Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point.

- ACL (Asynchronous ConnectionLess) – Data

  Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint.



Link manager protocol

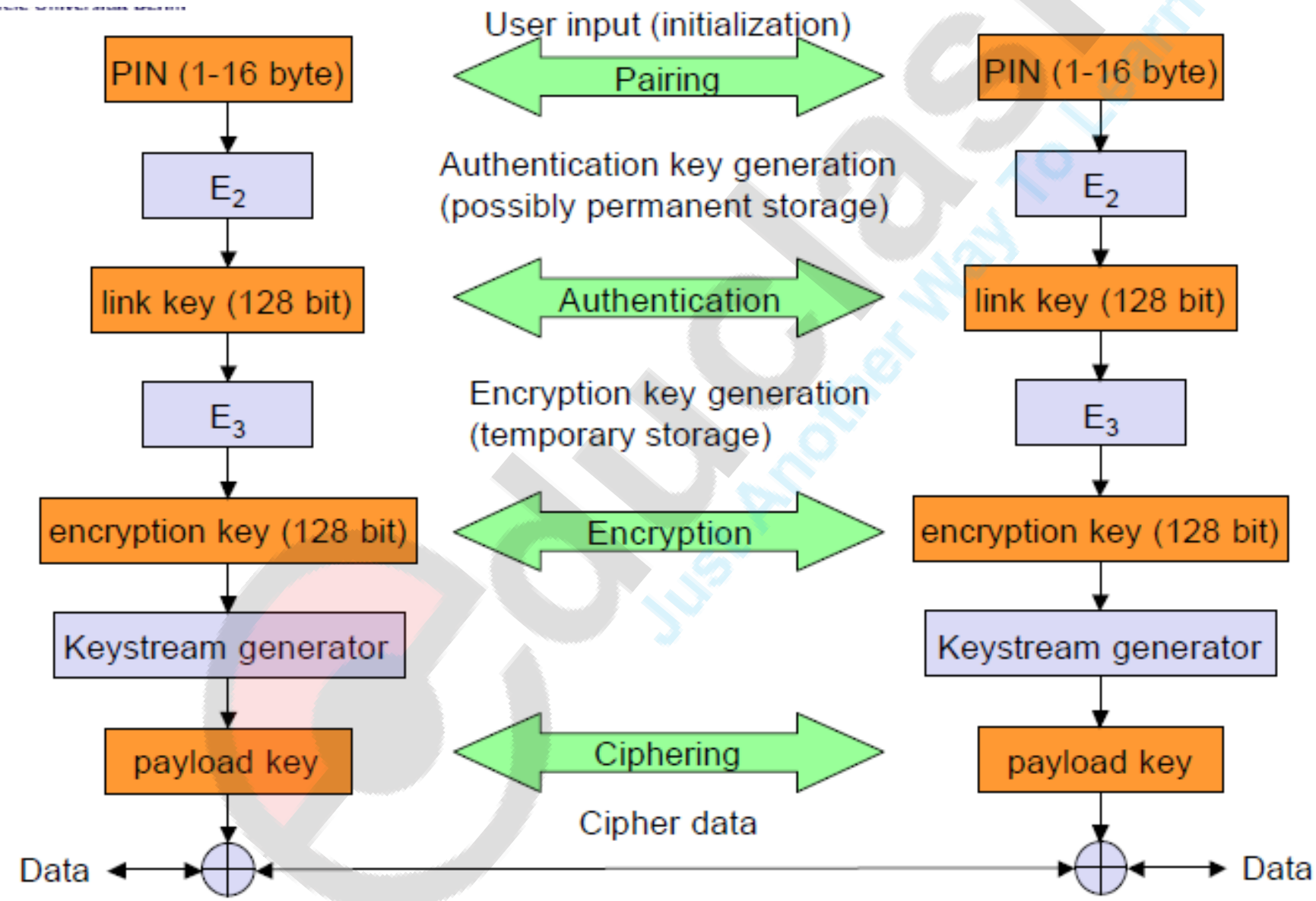
• manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices.
• LMP enhances baseband functionality, but higher layers can still directly access the baseband.

• Functions covered by LMP:
  - Authentication, Pairing and encryption.
  - Synchronization
  - Capability negotiation
  - Quality of service negotiation
  - Power control
  - Link Supervision
  - State and transmission mode change

L2CAP - Logical Link Control and Adaptation Protocol

- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signalling channels
- Protocol multiplexing
  - RFCOMM, SDP, telephony control
- Segmentation & reassembly
  - Up to 64kbyte user data, 16 bit CRC used from baseband
- QoS flow specification per channel
  - Follows RFC 1363, specifies delay, jitter, bursts, bandwidth
- Group abstraction
  - Create/close group, add/remove member

Security


User input (initialization)
PIN (1-16 byte)
Pairing
PIN (1-16 byte)
E_2
Authentication key generation
(possibly permanent storage)
E_2
link key (128 bit)
Authentication
link key (128 bit)
E_3
Encryption key generation
(temporary storage)
E_3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream generator
Keystream generator
payload key
Ciphering
payload key
Cipher data
Data
Data

SDP – Service Discovery Protocol

Inquiry/response protocol for discovering services

- Searching for and browsing services in radio proximity
- Adapted to the highly dynamic environment
- Defines discovery only, not the usage of services
- Caching of discovered services
- Gradual discovery

Additional protocols to support legacy protocols/apps

- RFCOMM
  - Emulation of a serial port (supports a large base of legacy applications)
  - Allows multiple ports over a single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
- OBEX
  - Exchange of objects, IrDA (Infrared Data Association) replacement
- WAP
  - Interacting with applications on cellular phones

Bluetooth Profiles

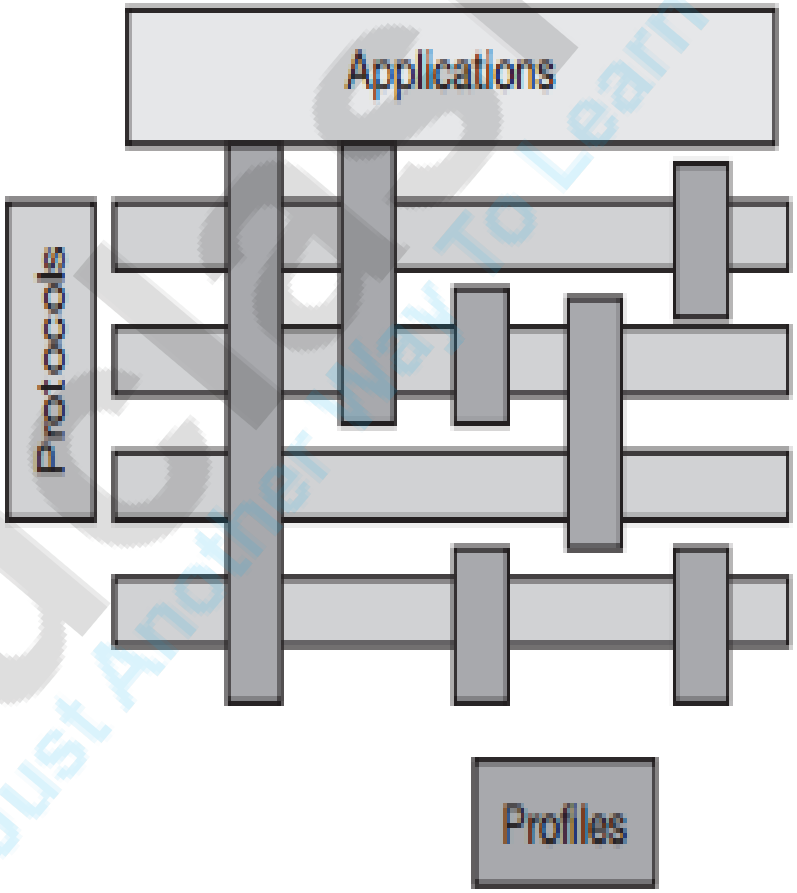
- Profiles represent default solutions for a certain usage model.
- They use a selection of protocols and parameter set to form a basis for interoperability.
- Protocols can be seen as horizontal layers while profiles are vertical slices

The following **basic profiles** have been specified: generic access, service discovery, cordless telephony, intercom, serial port, headset, dialup networking, fax, LAN access, generic object exchange, object push, file transfer, and synchronization.

Additional profiles are: advanced audio distribution, PAN, audio video remote control, basic printing, basic imaging, extended service discovery, generic audio video distribution, hands-free, and hardcopy cable replacement. Each profile selects a set of protocols.

For example, the serial port profile needs RFCOMM, SDP, LMP, L2CAP. Baseband and radio are always required. The profile further defines all interoperability requirements, such as RS232 control signals for RFCOMM or configuration options for L2CAP (QoS, max. transmission unit).

Figure 7.55
Bluetooth profiles



WPAN: IEEE 802.15-1 – Bluetooth

Data rate

- Synchronous, connection-oriented: 64 kbit/s
- Asynchronous, connectionless
  - 433.9 kbit/s symmetric
  - 723.2 / 57.6 kbit/s asymmetric

Transmission range

- POS (Personal Operating Space) up to 10 m
- with special transceivers up to 100 m

Frequency

- Free 2.4 GHz ISM-band

Security

- Challenge/response (SAFER+), hopping sequence

Availability

- Integrated into many products, several vendors

Connection set-up time

- Depends on power-mode
- Max. 2.56s, avg. 0.64s

Quality of Service

- Guarantees, ARQ/FEC

Manageability

- Public/private keys needed, key management not specified, simple system integration

Special Advantages/Disadvantages

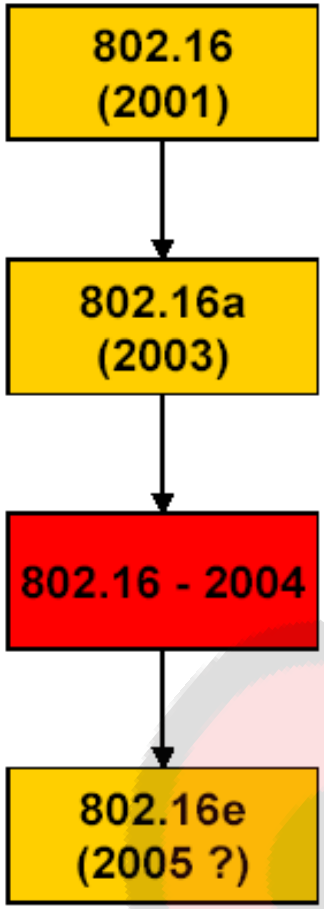
- Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
- Disadvantage: interference on ISM-band, limited range, max. 8 devices/network&master, high set-up latency

WiMAX- IEEE 802.16

WiMAX- IEEE 802.16

- WiMAX (Worldwide Interoperability for Microwave Access)
  - BWA (Broadband Wireless Access) Solution
  - Standard for constructing Wireless Metropolitan Area Networks (WMANs)
  - Can go to places where no wired infrastructure can reach
  - Backhauling Wi-Fi hotspots & cellular networks
  - Offers new and exciting opportunities to established and newly emerging companies
    - Incorporate cable (wired technology) standard
    - Comply with European BWA standard

IEEE 802.16 Evolution



- Fixed BWA at 10-66hz
- Line of sight

- Fixed BWA at 2-11hz
- None line of sight

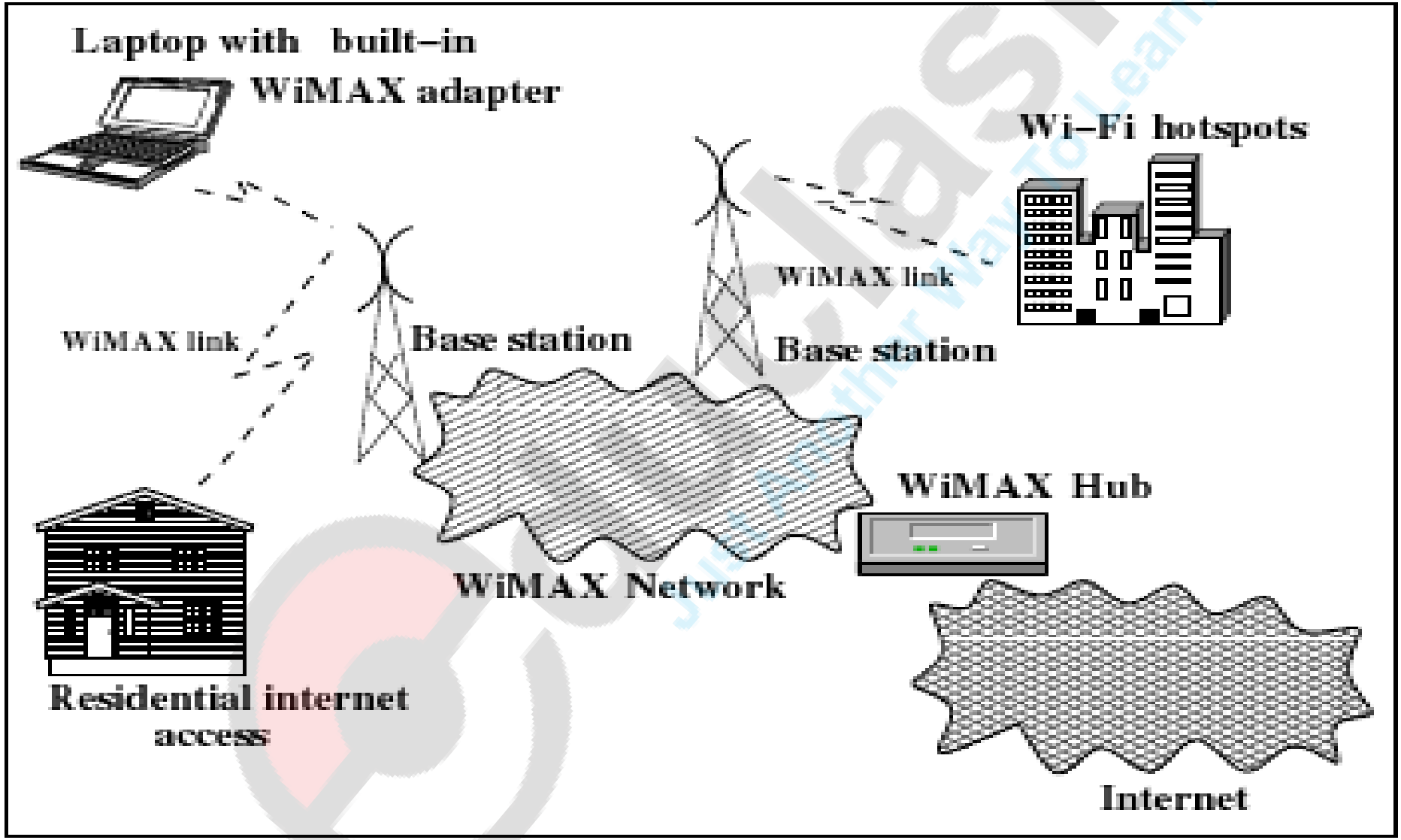
- Revision of 802.16
- Combine previous 802.16 standards

- Mobile BWA based on 802.16-2004 (802.16a)
- Roaming with vehicular speed

IEEE 802.16 Basics

	802.16a/REVd	802.16e
Completed	802.16a: Jan 2003 802.16REVd: Q3'04	Approved on Dec.7, 2005
Spectrum	< 11 GHz	< 11 GHz
Channel Conditions	Non line of sight	Non line of sight
Bit Rate	Up to 75 Mbps at 20MHz	Up to 75 Mbps at 20MHz
Modulation	OFDM 256 sub-carriers QPSK, 16QAM, 64QAM	OFDMA OFDM
Mobility	Fixed	Pedestrian mobility High-speed mobility
Channel Bandwidths	Selectable channel bandwidths between 1.25 and 20 MHz	Same as 802.16d with sub-channelization

WMAN Network Architecture



- Competes with both 3G wireless services and ISPs that distribute Internet access to fixed locations through telephone lines and cable television utilities.
- Subscribers usually use either a wired LAN or Wi-Fi to distribute the network within their buildings.

IEEE 802.16 Operation

WiMAX consists of two parts

A **WiMAX tower**, similar in concept to a cell-phone tower - A single WiMAX tower can provide coverage to a very large area -- as big as **3,000 square miles**.

A **WiMAX Receiver** The receiver and antenna could be a small box or PCMCIA card (Personal Computer Memory Card International Association), or they could be built into a laptop the way WiFi access is given.

Service Types

Non-Line-Of-Sight

A Service where a small antenna on your computer connects to the tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi).

Line-Of-Sight

A Service where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.

Architecture

P2MP (Point to Multi point)

» Wireless MAN

» BS connected to Public Networks

» BS serves Subscriber Stations (SS)

» Provides SS with first mile access to Public Networks

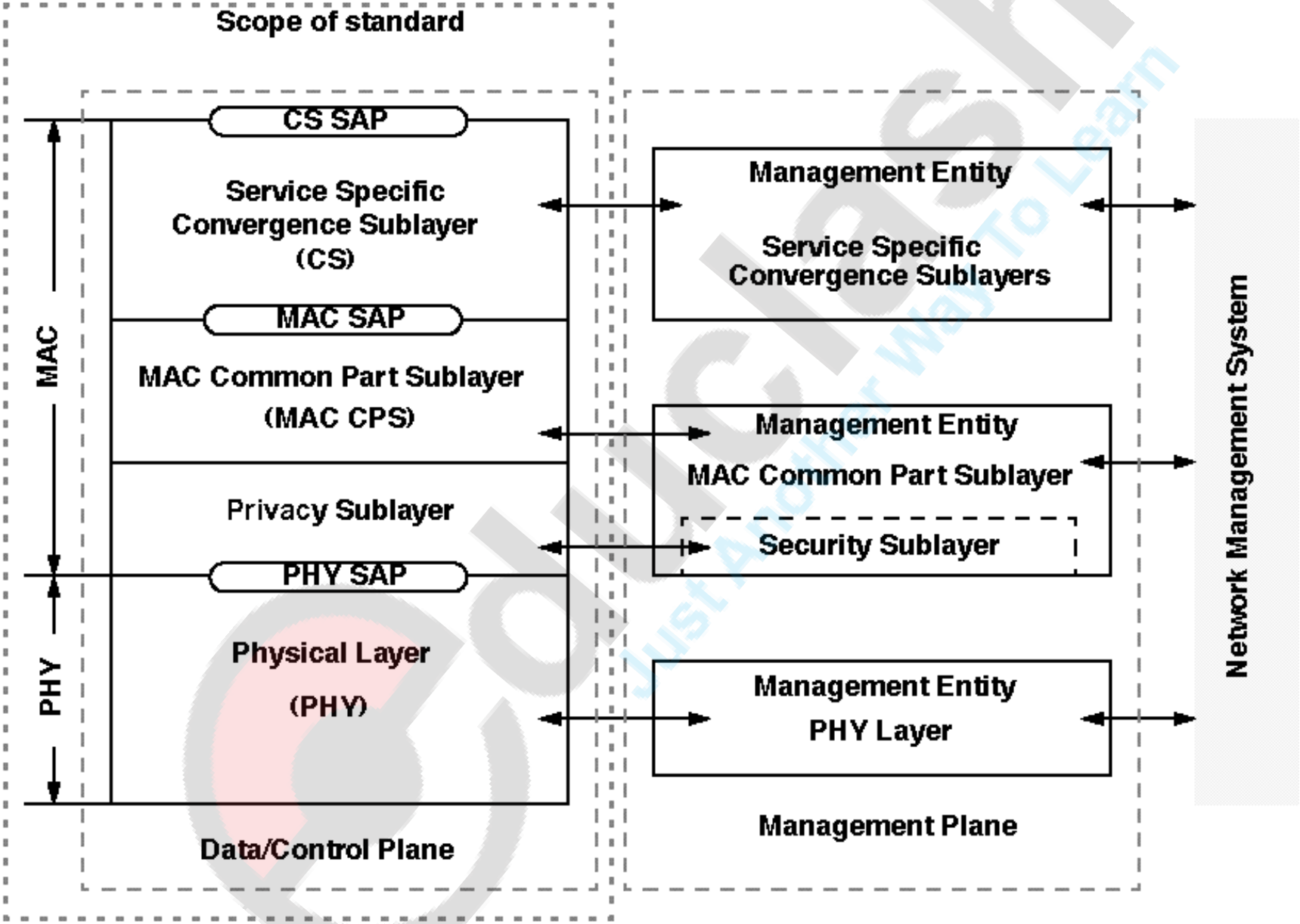
Mesh Architecture

» Optional architecture for WiMAX

Features of WiMAX

- Flexible Architecture
- High Security- using AES(Advanced encryption standard) and TDES (Triple data encryption standard).
- QoS- dynamic optimization in case of traffic.
- Quick deployment- little or no external plant construction.
- Multilevel services- service provider-service provider- subscriber
- Interoperability-easier to transport from one service provider to another.
- Portability
- Mobility using OFDM
- Cost effective
- Wider Coverage- using BPSK, QPSK, QAM
- NLOS operation
- High capacity- Higher bandwidth using QAM.

The 802.16 Protocol Stack



Physical Layer

- SOFDMA
- BW ranging from 1.25 to 20 MHz.
- Fixed sub carrier for both portable/mobile usage models.
- Scalable- sub channel with variable FFT sizes per channel BW.
- Multiple antenna support.
- Std band of frequencies:
  - 10-66 GHz
    - LOS operation
    - 120 Mbps data rate
  - 2-11 GHz.
    - LOS and NLOS operations
- Allows use of directional antennas

  Improves range
- Allows use of two different duplexing schemes:

  Frequency Division Duplexing (FDD)

  Time Division Duplexing (TDD)
- Support for both full and half duplex stations.

MAC Layer

- 3 sub layers
  - **Service specific convergence sub layer (CS)**
    - Gets higher level data through SAP(service access point)
    - Provides transformation and mapping into MAC SDU
  - **MAC common part sub layer (CPS)**
    - Receives SDU(service data unit) through SAP
    - 2 types of transformations- ATM and Packet
    - Core part of MAC layer
    - Defines MAC
    - Duplexing and channelization
    - Channel access
    - Packet data unit (PDU) framing
    - Network entry and initialization
    - QoS
    - BW allocation
    - Connection maintenance
  - **Privacy sublayer**
    - Encryption and decryption (to and from PHY layer)
    - Authentication and secure key exchange.

MAC Addressing

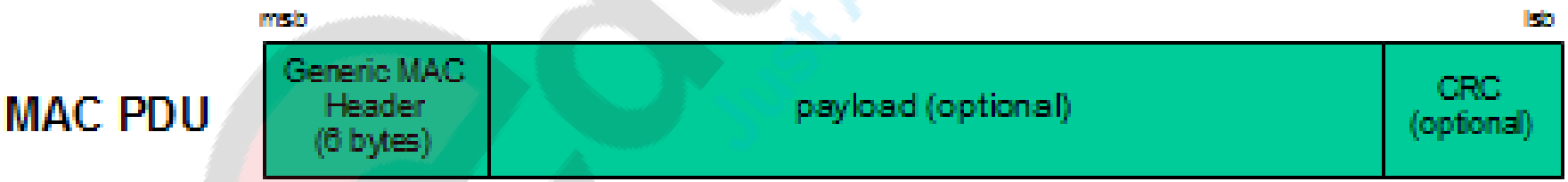
- SS has 48-bit 802.3 MAC address
- BS has 48-bit base station ID
  - » Not a MAC address
- Connection ID (CID)
  - » 16 bit
  - » Used in MAC PDU
  - » Connection Oriented Service

Sub-channelization

- A single user can use all sub carriers at any given time.
- Subsets of sub carriers are assigned to multiple users allowing number of subscribers to be served simultaneously.
- Specific carrier groups are used for each subscriber.
- Subcarrier assignment- dynamic- to overcome multipath interference.
- Allows to group a no. of OFDM carriers into blocks which can be assigned to different WiMAX BS sector.

MAC PDU

- Each MAC packet consists of the three components,
- » A ***MAC header***, which contains frame control information.
- » A variable length ***frame body***, which contains information specific to the frame *type*.
- » A ***frame check sequence*** (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).



References

[1] Wireless and Mobile Networks, Concepts and Protocols, Dr. Sunilkumar S.Manvi, Mahabaleshwar S. Kakkasageri, Wiley India.

[2] Mobile Communications, Second Edition, Jochen Schiller, Pearson Education.

[3] Wireless Communications & Networks, Second Edition, William Stallings, Pearson Education.

Reference books (Topic-wise)

Sr. No.	Topic	Ref. Book	Chapter No.
1	Wireless network, Wireless network Architecture,	Wireless and Mobile Networks, Concepts and Protocols, Dr. Sunilkumar S.Manvi, Mahabaleshwar S. Kakkasageri, Wiley India	2
2	Classification of wireless networks – WBAN, WPAN, WLAN, WMAN, WWAN.	Wireless and Mobile Networks, Concepts and Protocols, Dr. Sunilkumar S. Manvi, Mahabaleshwar S. Kakkasageri, Wiley India	2
3	IEEE 802.11	Mobile Communications, Second Edition, Jochen Schiller, Pearson Education	7
4	IEEE 802.16	Wireless and Mobile Networks, Concepts and Protocols, Dr. Sunilkumar S. Manvi, Mahabaleshwar S. Kakkasageri, Wiley India	6
5	Bluetooth – Standards, Architecture and Services	Wireless and Mobile Networks, Concepts and Protocols, Dr. Sunilkumar S. Manvi, Mahabaleshwar S. Kakkasageri, Wiley India OR Wireless Communications & Networks, Second Edition, William Stallings, Pearson Education	4 OR 15

University Questions

1. What are piconet and scatternet? Explain the various protocols supported by Bluetooth protocol architecture.- May 16- 7M
2. Describe |EEE 802.11 Architecture.- May 16- 8M
3. Short note on WiMAX.-May 16- 5M
4. Explain with the state diagram how the bluetooth devices changes from the standby state to the active state.- Nov 16- 7M- Refer page 522, chapter 15, William Stallings.
5. Explain the IEEE 802.11 architecture with diagram. Discuss the services provided by IEEE 802.11.- Nov 16-8M.
6. Explain the IEEE 802.16 architecture with services provided.- Nov 16-7M.