Wireless LAN and Personal Area Network Protocols

Lesson 05

Bluetooth

Bluetooth

- Derived from the name of a Danish king
- The king Harald Blatand which means Bluetooth in English reigned before 1000 A.D.
- Bluetooth is a protocol used in WPAN (Wireless Personal Area Network)

WPAN

- Consists of Bluetooth **Piconets and scatternet**
- Piconet– Bluetooth devices network with maximum eight devices within a distance of about 10 m
- Scatternet– an ad-hoc network formed by various piconets within 100 m through a Bluetooth-enabled bridging device

Bluetooth Features

- Used for low power short range transmission
- Bluetooth radiations between piconets are omnidirectional

Bluetooth Features

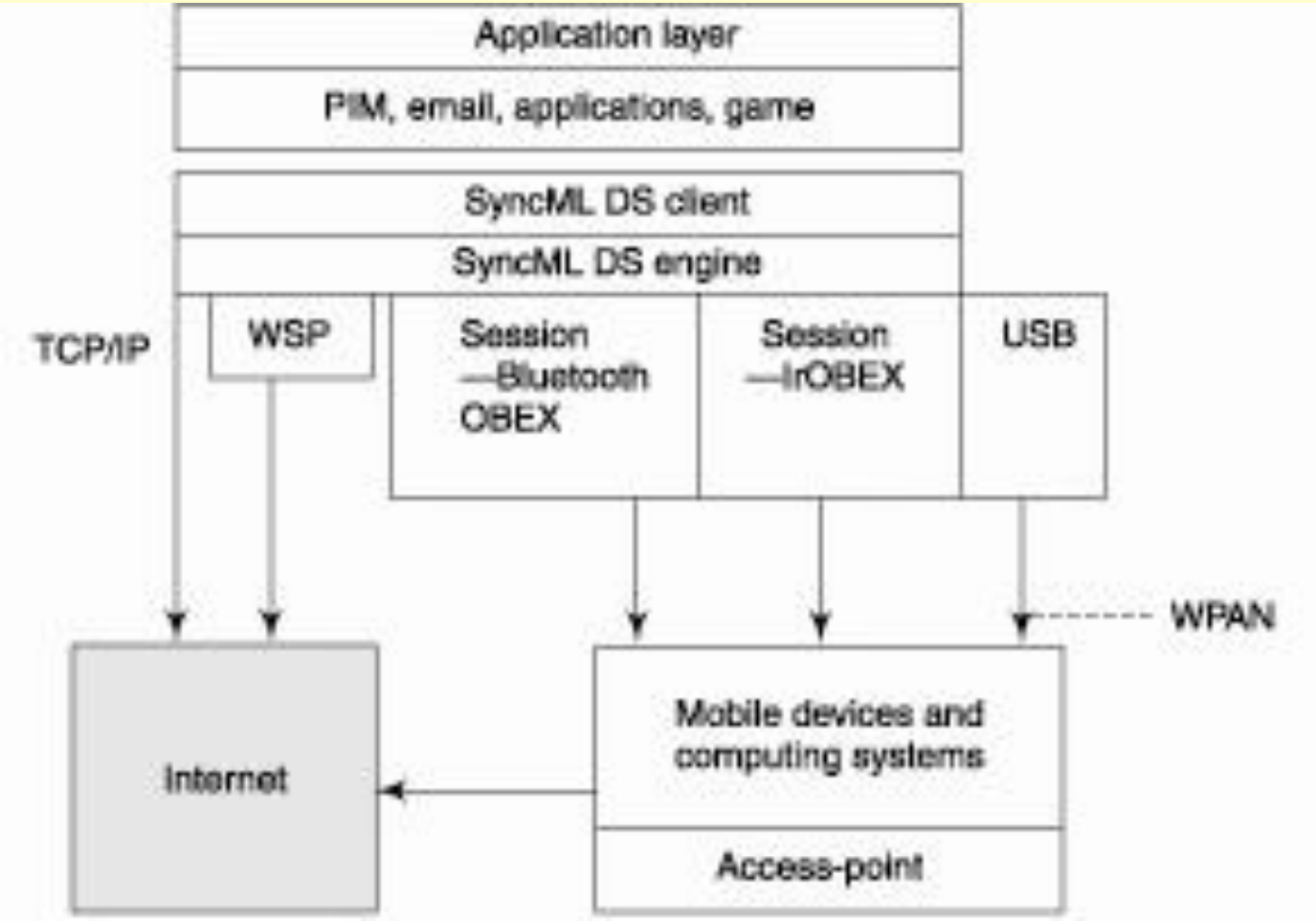
- Network connection latency—3 s
- Bit rate—less than 1 Mbps; Bluetooth 3.0 HS version 24 Mbps data transfer rate at 10 m range,

  Bluetooth 4.0 version 24 Mbps data transfer rate, and can be up to 60 m range (depending on the device)

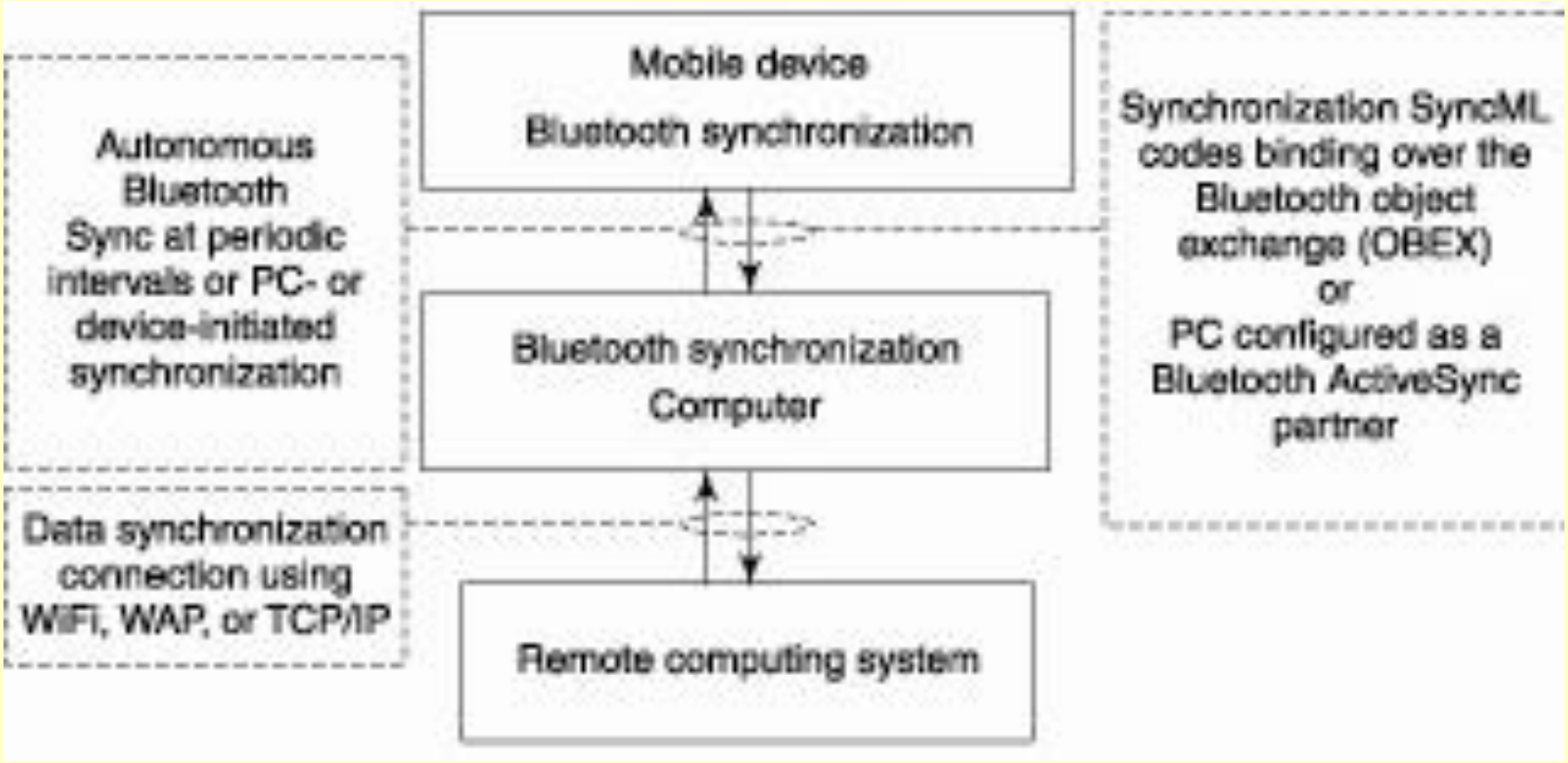
Bluetooth Features

- Protocol stack—larger than IrDA or Bluetooth
- Code size—2 to 50% more compared to that for a Zigbee device
- Bluetooth radio—FHSS

Data synchronisation between the mobile devices and computing systems in a WPAN



Synchronisation of remote system with the Bluetooth devices



Bluetooth devices network

- Any device can function as master or slave
- The device which first establishes a piconet becomes master and others which discover the master become slaves in the piconet
- Slave means that the clock of the master functions as reference for synchronization

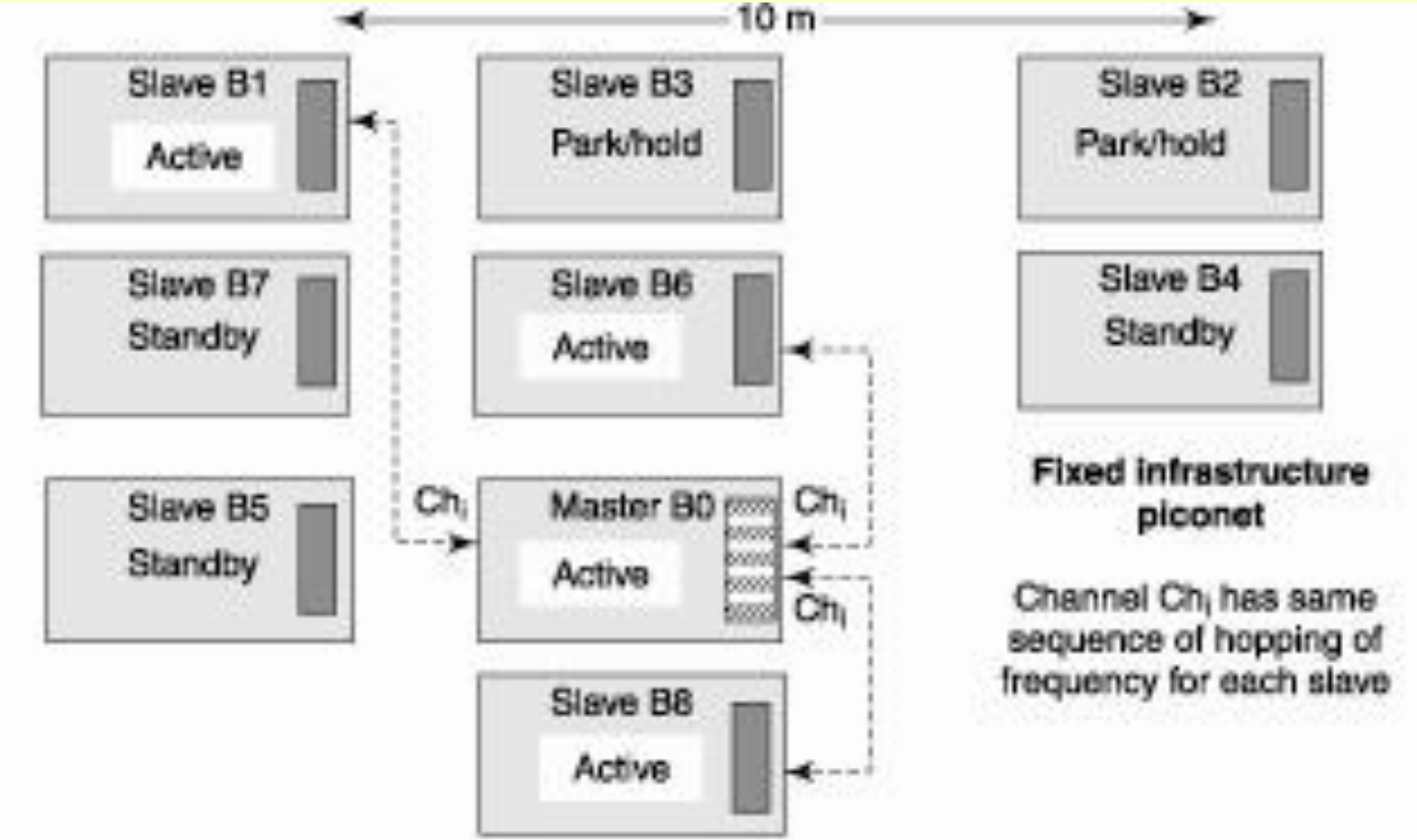
Master

- Synchronizes all active devices and there are identical hopping sequences of their frequencies for each device's radio (transmitter)
- A hopping sequence defines one channel
- There can be a maximum of eight devices with a master in piconet and a maximum of 79 channels in Bluetooth networks

Example of Piconet of 3 active Bluetooth devices and a master

- Each device synchronised and using same hopping sequence of their frequencies forming a fixed infrastructure network architecture
- Two are in park/hold state and Three are in standby mode

Piconet of 3 active Bluetooth devices and a master



State of devices in a piconet

- Standby
- Active
- Park
- Hold
- Sniff

Standby

- Waiting to discover the master and thus the piconet
- No RF signal communication is taking place)
- Device is yet to be assigned an address in the piconet

Active state– one of the three modes

(a) Inquiring– (carrying out discovery broadcasting in all neighbourhood and listening to the response for finding out a radio channel to connect

(b) Paging – sending a page specifying the relationship with master after discovering the channel

Active state– one of the three modes

(c) Connected and performing data transactions–

- When a device is discovered and becomes an active device
- 3 bit address called AMA (active member address) assigned by the master device
- 000 reserved for use when a broadcast to all active devices takes place

Active state device

- Listens the data in the piconet at short intervals
- The messages are transmitted sixteen hundred times in one second

Park state

- Device already discovered the piconet
- But not communicating at present
- Is held in power-saving mode
- Assigned a 3 bit address called PMA (parked member address) after being released of the AMA
- Retained as a member of piconet
- To save power, it reduces duty cycle of the bit rate (clock frequency)

Hold state

- Hold state retains the AMA but suspends asynchronous connectionless link (ACL)
- It maintains synchronous connection oriented (SCO) link
- Reduces power dissipation for communication in this piconet when there are no packet exchanges with the master

Sniff state

- Retains the AMA
- Operates at high power level
- Sniffing means listening to the existing Bluetooth device in the vicinity
- Sniffs the data of communicating piconet at large programmable intervals as compared to active state short intervals

Example

1. At t_0: A Bluetooth device B0 discovers a device B1 within 10 m
2. At t_1: Then the devices B2, B3, B6, and B8 also reach within 10 m and join the network

Example

- At t_2: After some time, since B2 and B3 are not exchanging objects, they go to park state to save the power
- At t_3: After some time, the devices B7, B5, B4, B9, and B10 move in sequence within 10 m but they have to discover the network

The states, devices, AMAs, PMAs in the piconet

- After t_0: B0 will function as master in the piconet as it first discovered the device B1 in its vicinity
- After t_1: Slaves B1, B6, and B8 will be in active (either inquire, page, or connected) states, master can assign AMAs 001, 100, and 111

The states, devices, AMAs, PMAs in the piconet

- After t_2: Slaves B2 and B3 are in park state, PMAs can be 001 and 010
- After t_3: B7, B5, and B4 are in standby mode waiting to discover the service network, yet to be assigned member address by the master

Other piconet outside the Piconet

- B9 and B10 cannot be a part of this piconet and will form another piconet operating at another channel with another sequence of frequency hops

Master and slave devices moving out to another piconet

- Master becomes slave in a new piconet
- When it moves to another established piconet, the communication in the previous piconet freezes

Master and slave devices moving out to another piconet

- The device which rediscovers another device then becomes master in the previous piconet
- When a slave moves to another area, it communicates its unavailability to its master
- It then synchronizes with a new piconet

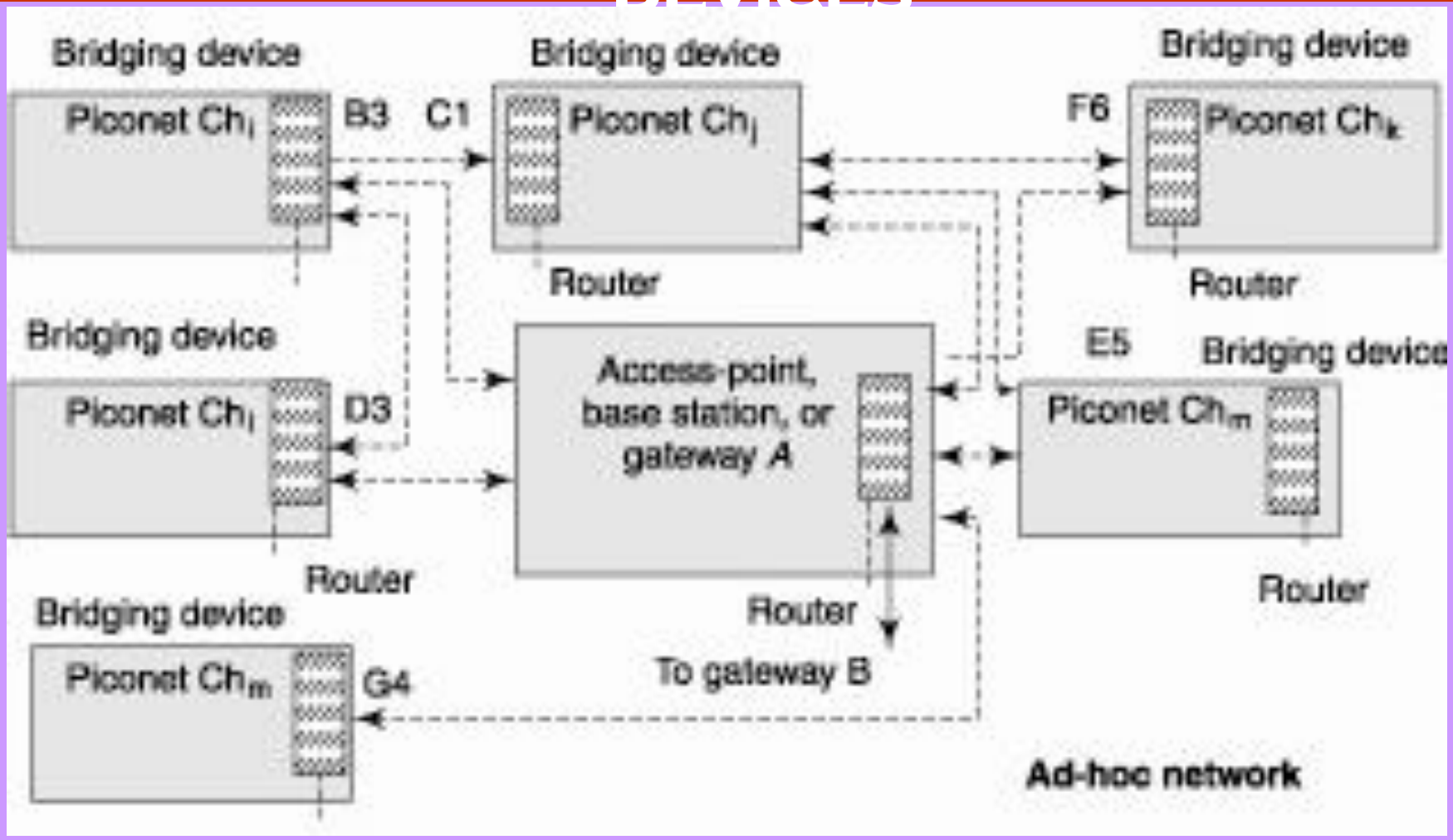
Scatternet

- An ad-hoc network formed by the bridging devices
- A bridging device connects two piconets
- Any Bluetooth device can function as a bridge in order to form the ad-hoc network
- In such a network, two devices in two piconets communicate as in a peer-to-peer communication

Scatternet

- The two devices use two different channels (two different hopping sequences from among the 79 provided)
- Each piconet uses FH-CDMA so that there is a distinct hopping sequence with respect to other piconets in the scatternet
- Therefore, there are no collisions between signals in two piconets

Bluetooth devices ad-hoc network (scatternet) through bridging devices



Ad-hoc network architecture of Bluetooth-enabled devices

- Formed by the bridging devices
- Six piconets consisting of the devices B0, …, B7, C0, …, C7, D0, …, D7, E0, …, E7, F0, …, F7, and G0, …, G7
- Scatternet forms with B3, C1, D3, E5, F6, and G4 as bridging devices

Bluetooth protocol IEEE 802.15.1 specifications

- A Bluetooth device has number of protocols that can be used at the application, presentation, session, transport, network, data link, and physical layers (layers 7-1)

Protocols at the application layer

- vCard
- vCal
- Telephonic network protocol
- Device management protocol
- SyncML, SyncML Client, SyncML Engine

Functions of Protocol Layers

Application
- vCard, vCal-telephonic
- Network
- Device management, SyncML client, engine
- Modem commands to RFCOMM serial

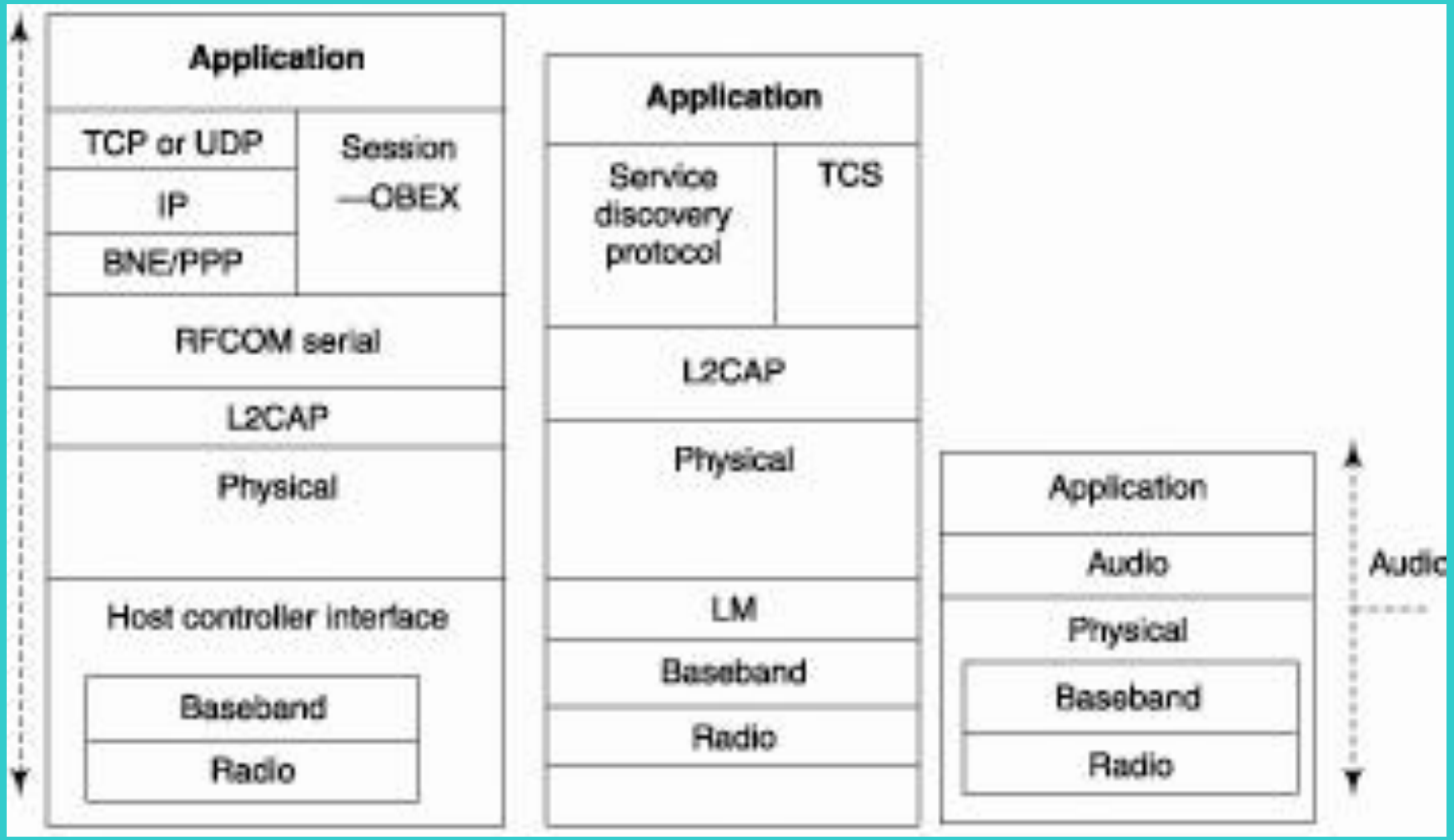
TCSP
- Telephony control specification protocol

BNEP
- Bluetooth network encapsulation protocol

Baseband
- Fast FHSS algorithm
- Establishment of connection
- Packets formation
- Timing control for synchronization
- Basic QoS maintenance

L2CAP
(logical link control and adaptation protocol)
- Multiplexing data of higher layer protocols.
- Segmentation and reassembly of packets.
- Transmission management to a group of devices.
- Communication over the host ACL
- QoS management

Host protocol layers and other protocol layers between the object client, device and server



Physical layer

- Responsible for transmitting header fields encapsulating the payload and payload
- Payload– means data to be transmitted after passing through the layers 7 to 2 and retrieved at other end after passing through layers 2 to 7

Bluetooth device physical layer has three sub-layers

- Link manager or host controller interface– sub-layer responsible for interfacing with the upper layers
- Baseband– another sub-layer generates the baseband signal used for transmission
- Radio – Another generates the radio signals as per the data bits from or for the MAC (layer 2)

Radio

- Transmits packets received from baseband sub-layer
- At the other end of the link, it receives
- Operate at the least required power levels so that the transactions may not be detected by a distant receiver of signals, thus maintaining confidentiality

Radio

- Frequency hopping CDMA ensures negligible interference and least risk of jamming by distant sources

Radio Sub-layer characteristics

- Frequency band– 2.4 GHz
- Maximum power levels for devices – 1, 2, or 3 corresponding to 100 mW, 2.5 mW, or 1 mW

Radio Sub-layer characteristics

- Bluetooth radio — FHSS with each carrier separated by 1 MHz, 1600 frequency hops per second among 79 carriers, and frequency changing after every 1/1600 s or 625 μs
- Transceiver modulation— GFSK

Radio Sub-layer characteristics

- Data transfer rates — 1 Mbps or less
- Range — 10 m in a piconet and 100 m in a scatternet
- Baseband— uses a fast frequency hopping algorithm and after 625 μs, the frequency of a channel changes according to a code which defines the sequence in which the carrier frequency has to change

Baseband Two types of links two between Bluetooth devices

- ACL (asynchronous connectionless link)
- SCO (synchronous connection oriented) link
- ACL link provides best effort traffic
- SCO links provide real-time voice traffic using reserved bandwidth

Baseband Packet

- Of about 350 bytes and has a payload of 2744 bits or 343 bytes, b0-b2743
- It has 68 bits access code plus 4 bit trailer to access code (or alternatively 72-bit channel access code) at the beginning
- It is followed by a 54 bit packet header
- Packet deploys FEC for correcting the transmission errors [refer Section 12.5.1.2]

Link Manager

- Baseband and radio provide a link between master and slave
- The functions of the link manager—

(i) supervision

(ii) monitoring of power, synchronization, state, and mode of transmission,

Link Manager

(iii) exchange of QoS parameters (for example, packet flow latency, peak data rate, average data rate, and maximum burst size) for L2CAP and higher layers and capability information exchange

(iv) handling device pairing

(v) handling data encryption and device authentication

- Table 12.3 for details [Refer section 12.5.1.3]

Bluetooth host-controller interface (HCI)

- Manages the link between the upper layer and baseband and radio sub-layers of the physical layer
- It is hardware abstraction layer in place of link manager

Bluetooth host-controller interface (HCI)

- Host controller interface (HCI) interfaces RF communication serial [3 wire UART (universal asynchronous receiver and transmitter) which is an RS232 emulation in RF communication] line and mode through L2CAP software layer

MAC LAYER

- Data link control carried out using L2CAP
- L2CAP– to provide logical link control and provide an adaptation mechanism using Bluetooth
- Passes the segmented or reassembled packets directly to the link manager or HCI in case of host-controller-based system

A LOGICAL-LINK ADAPTAION-REQUEST

- Received from upper layers at client device
- Then multiplexed and segmented as per available maximum transferable units (MTUs) at the baseband
- After this, the logical link adaptaion confirmation sent to higher protocol layers

A logical-link adaptaion-request

- Then a link program request is sent to lower layer HCI or LM
- The link program protocol confirmation is then received back at L2CAP layer

L2CAP

- Facilitates segmentation of packets while transmitting and reassembling of packets on reception
- Multiplexes the data between different higher layer protocols and manages forward transmission from a Bluetooth device to other devices

L2CAP

- Does QoS management for higher layer data
- [A program file needs error free transfer. A picture being transferred can contain errors but still look good. It means ensuring the expected level of service.]
- Provides connection-establishment-based communication after a host ACL is established

L2CAP THREE LOGICAL CHANNELS

(i) signalling messages between L2CAP at transmiiter and receiver devices

(ii) bi-directional connection-oriented with support for QoS parameters from higher layers, and

(iii) unidirectional connectionless broadcast from master to slave

Summary

- Bluetooth device number of protocols that can be used at the application, presentation, session, transport, network, data link, and physical layers (layers 7-1)
- Physical layer three sublayers: radio, baseband and Link manager or HCI
- MAC layer L2CAP
- Three logical channels

Summary

- Bluetooth devices network
- Piconet– within about 10 m
- Standby, Active, Park, Hold, Sniff states
- Scatternet– an ad-hoc network formed by various piconets within 100 m
- Bridging Devices between the piconets

…

...Summary

- Any device can function as master or slave, first establishing device in a piconet becomes master
- Maximum of eight devices with a master in piconet
- Maximum 79 channels in Bluetooth network

End of Lesson 05

Bluetooth