Wireless Networks

Dr. Tuhina Samanta

Wireless Networks

- New handheld devices come into the market
- Wireless indoor: Wireless LANs come into existence: in office premises, buildings, multistoried markets
- Wireless outdoor: concerned with WLL technology: realizes Wireless Metropolitan Area Network (WMAN)
- Big antennas are required with directed antenna at the user end
- Two configurations of WLAN: With base station, without base station
    - Both operate in short range radio wave communication

Wireless LAN

Challenges: (1) Finding an available frequency band

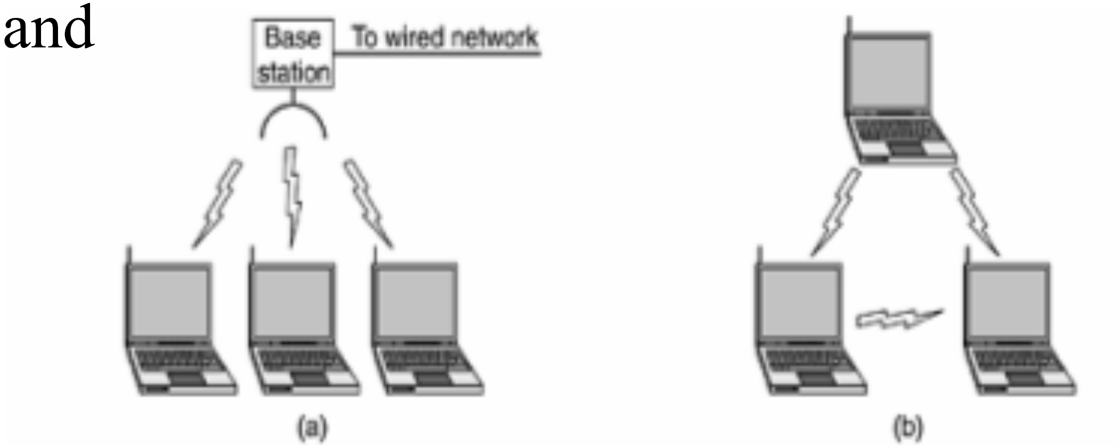
(2) Finite range of signals

(3) user privacy

(4) Limited battery life

(5) Mobility

(6) Making the system economically viable



Wireless LANs that operate without base stations are called Mobile Ad hoc NETworks (MANETs)

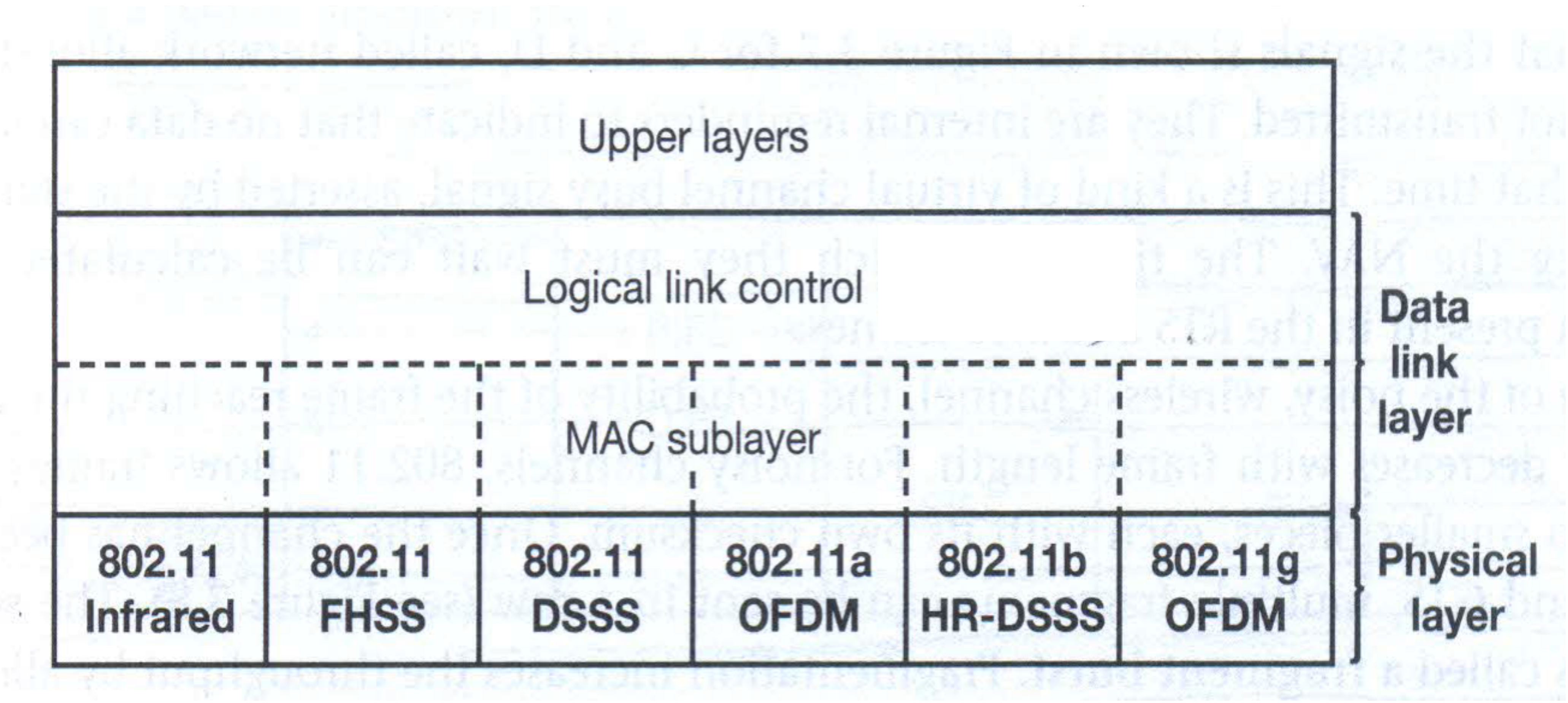
Need of New Wireless Standards

- Why can’t the standard Ethernet be used in WLAN?
- Ethernet uses CSMA/CD: hidden and exposed stations problem
- Multipath fading occurs
- No handfoff
- Half duplex transmission
- Absence of mobility-aware software

IEEE 802.11 WLAN standard

- Popularly known as Wi-Fi standard
- Data rate at Physical layer is 1-2 Mbps for WLAN
- Data link layer consists of two sub layers
    - Logical link control (LLC)
    - Medium access control (MAC)

Lower Layers of 802.11 Protocol Stack



Upper layers

Logical link control

MAC sublayer

802.11 Infrared

802.11 FHSS

802.11 DSSS

802.11a OFDM

802.11b HR-DSSS

802.11g OFDM

Data link layer

Physical layer

Physical Layer

- 802.11: Infrared transmission, 1-2 Mbps data rate. Infrared signal does not penetrate wall, but not good in sunlight, limited bandwidth
- 802.11: FHSS, uses 79 channels, each 1 MHz wide, starting at the low end of 2.4 GHz ISM
  - FHSS provided security against eavesdropping, less immune to multipath fading and radio interference, hence good for wireless outdoors
  - Disadvantage is low bandwidth and low power
- 802.11: DSSS, restricted to 1-2 Mbps, uses 11 chips Barker Sequence, phase shift modulation is used
- 802.11a: OFDM, 5 GHz. ISM frequency band, 54 Mbps data rate, 52 different frequencies are used
- 802.11b: HR-DSSS, 11 million chips per second, data rate 11 Mbps in the 2.4 GHz. Band
- 802.11g : Uses OFDM and frequency band of 802.11b, upto 54 Mbps data rate

MAC Layer

To overcome hidden and exposed stations problem in CSMA/CD based Ethernet, MAC sublayer of 802.11 supports two modes of operations, DCF and PCF

- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)

Distributed Coordination Function (DCF)

This mode does not use any central control, like the Ethernet. But it uses CSMA/CA, i.e., CSMA with Collision Avoidance, which itself supports two methods of operation

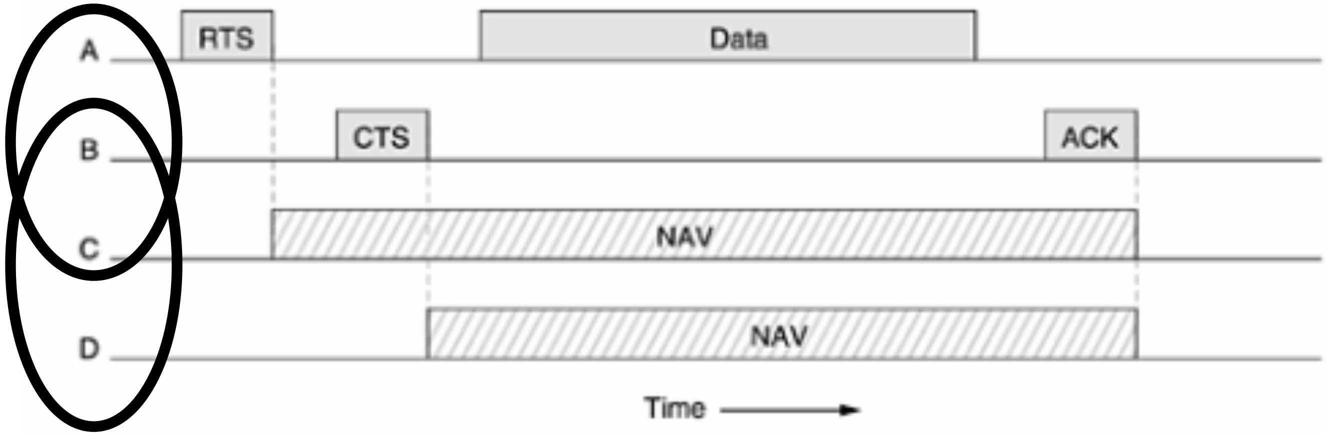
a) The first method uses physical channel sensing:

    a) When a station wants to transmit, it senses an idle channel, finds it and send data. If a collision occurs, the colliding stations wait for a random time using Ethernet binary exponent backoff (BEB) algorithm and try again later. If the receiver does not send and acknowledgement, the transmitter knows that a collision has occurred. There is no collision detection at the transmitter

b) The second method is based on Multiple Access with Collision Avoidance for Wireless (MACAW) and uses virtual channel sensing.

Multiple Access with Collision Avoidance for Wireless (MACAW)

- A sends a 30 byte RTS (request to send) frame to B
- If B is ready CTS (clear to send) frame is sent by him
- A receives CTS, sends data frame and starts ACK timer
- Upon completion of data B responds to the ACK frame and terminates exchange
- Is A’s ACK timer expires before receiving ACK from B, the whole process is repeated
- C receives RTS and stops transmission, D receives CTS and stops transmission

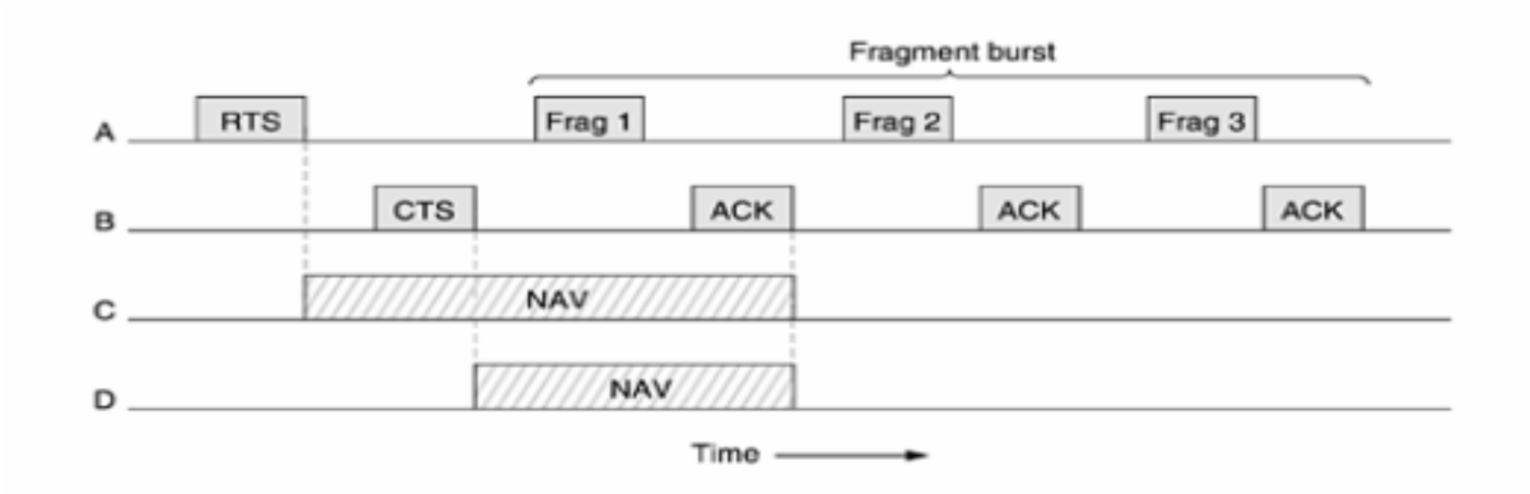


NAV—> Network allocation vector
This is a virtual channel busy signal
asserted by C and D

Virtual channel sensing using CSMA/CA

Fragmentation

- Because of the noisy, wireless channel, the probability of the frame making successfully, decreases with frame length.
- To deal with the problem of noisy channels, 802.11 allows frames to be fragmented into smaller pieces ,each with its own checksum.



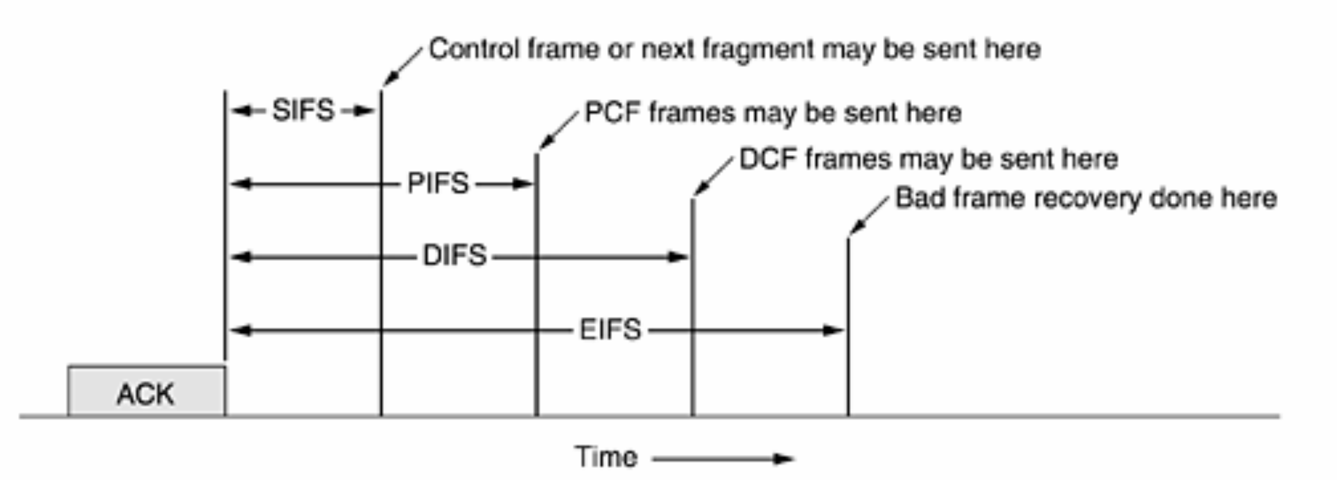
A fragment burst in IEEE 802.11

Point Coordination Function (PCF)

- This mode uses a central, the base station, which polls the other stations, asking them if they have any frames to send.
- No collisions can occur.
- The base station broadcasts a **beacon frame** periodically, with the necessary system parameters, viz., hopping sequence, dwell times, clock synchronization, etc.

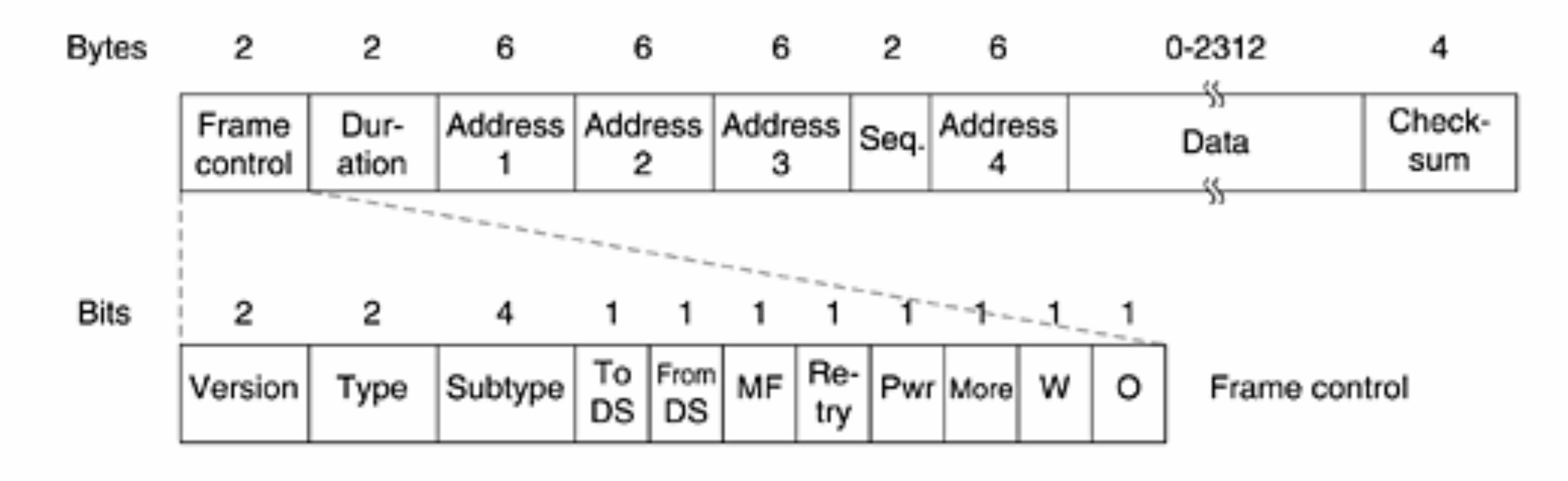
Both PCF and DCF can coexist within one cell. After a frame has been sent,

a certain amount of dead time is required before any station may send another frame.


Control frame or next fragment may be sent here
SIFS
PCF frames may be sent here
PIFS
DCF frames may be sent here
DIFS
Bad frame recovery done here
EIFS
ACK
Time

IEEE 802.11 Interframe spacing

IEEE 802.11 **Frame Structure**



Bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Duration	Address 1	Address 2	Address 3	Seq.	Address 4	Data	Checksum

Bits	2	2	4	1	1	1	1	1	1	1	1	
	Version	Type	Subtype	To DS	From DS	MF	Retry	Pwr	More	W	O	Frame control

Data Frame format for IEEE 802.11

Management frames have similar format, except without one of the Base addresses, because they are restricted to a single cell.

Control frames are shorter, having only one or two addresses, no *data* and *sequence* fields. *Subtype* is important here.

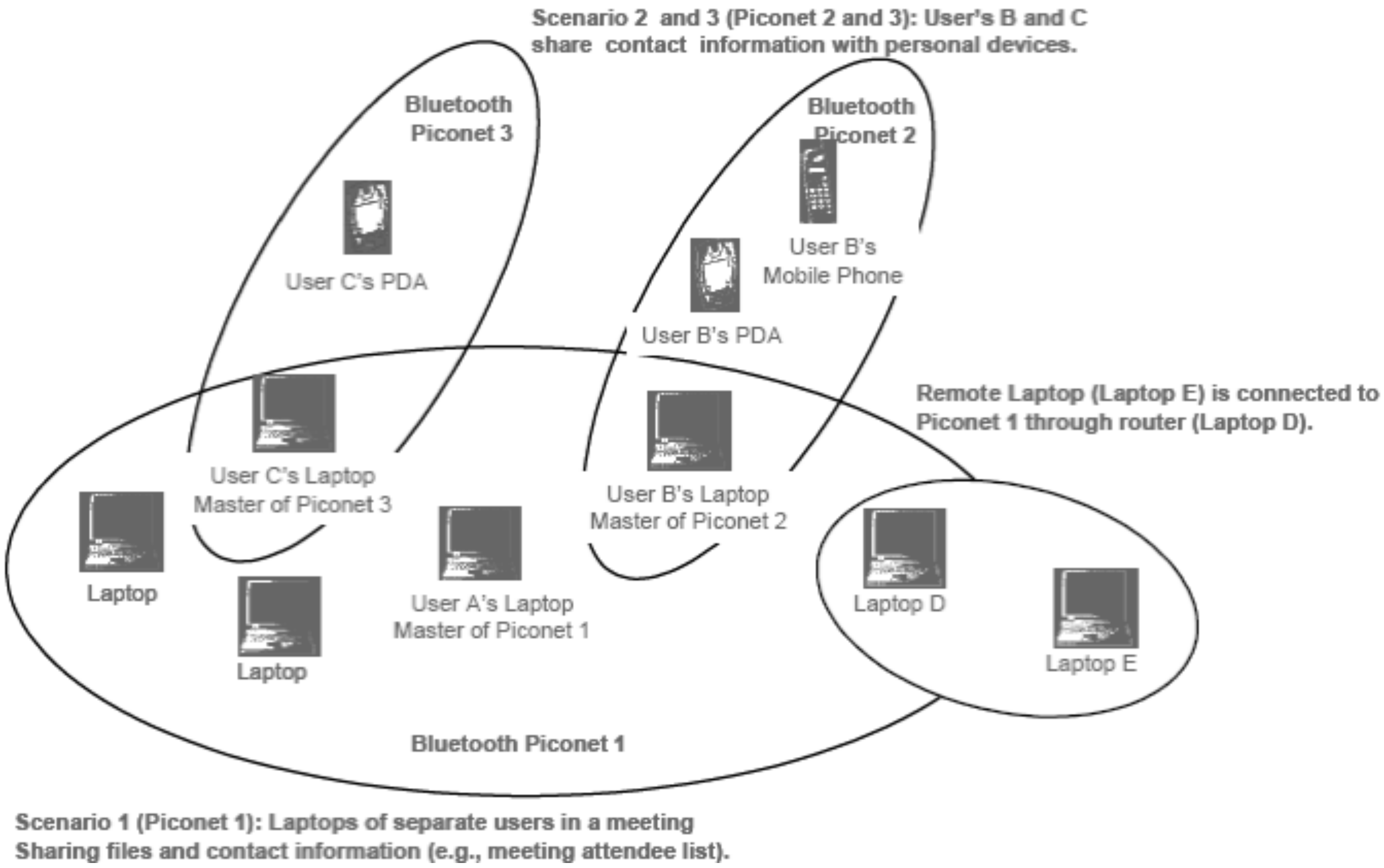
Services

A wireless LAN must provide nine types of services, divided into two categories: five distribution services and four station services.

- The five **distribution** services relate to managing cell membership and interacting with stations outside the cell. They are as follows:
  - Association
  - Disassociation
  - Re-association
  - Distribution
  - Integration
- The four station **services** relate to activity within a single cell. They are used after association has taken place and are as follows:
  - Authentication
  - De-authentication
  - Privacy
  - Data delivery

BLUETOOTH

- Bluetooth was developed for connecting mobile phones or computing and communication devices. In 2002 it was taken as the IEEE 802.15 standard, for the physical and data link layers.
    - It is a short range, low cost and power efficient radio-frequency based wireless technology
    - Supports both point-to-point and point-to-multipoint connections
    - Connects devices with active Bluetooth within 30 feet or 10 meter radius
    - Eight devices can be connected in a network, known as Piconet

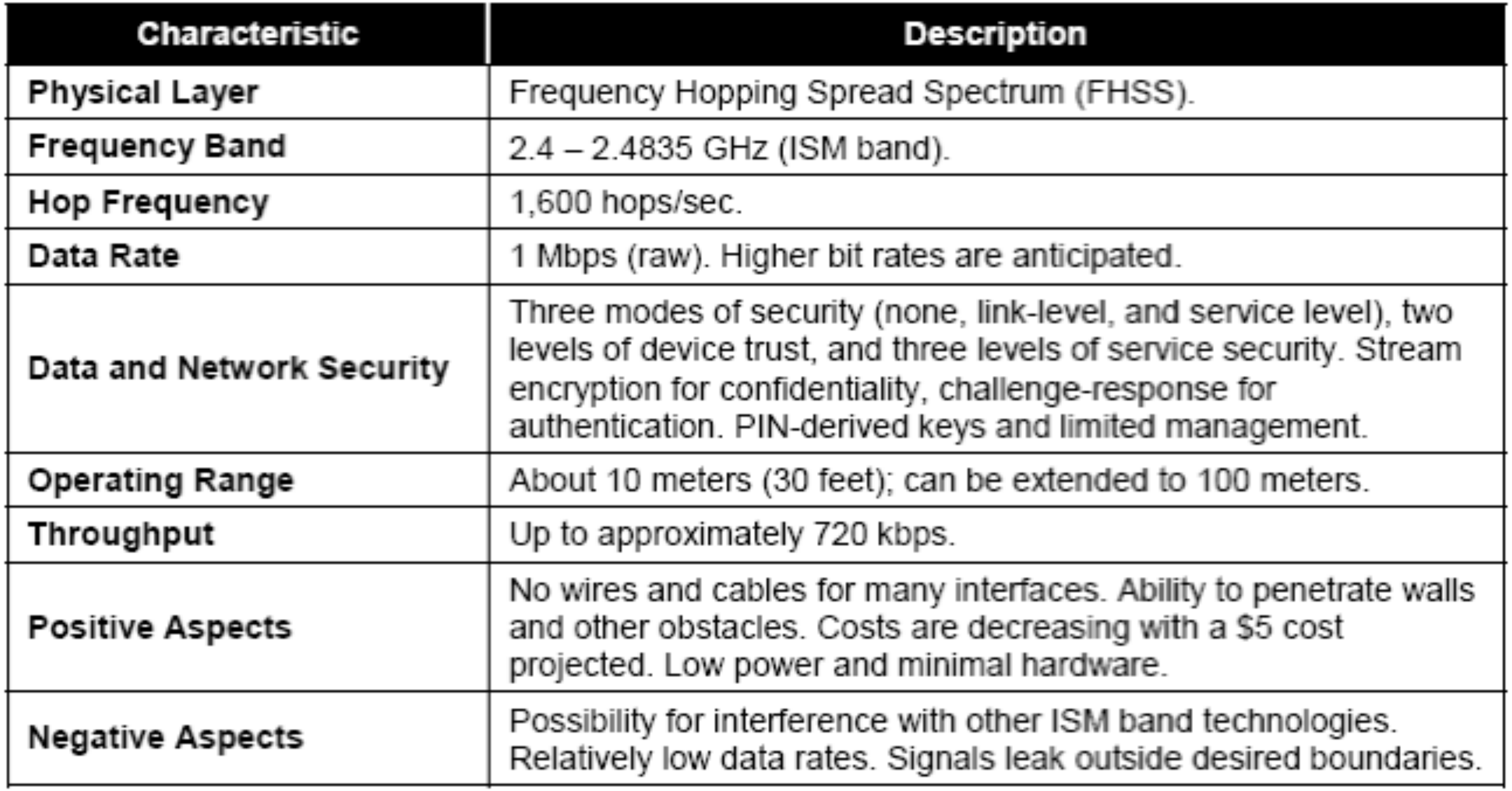


Scenario 2 and 3 (Piconet 2 and 3): User's B and C share contact information with personal devices.
Bluetooth Piconet 3
Bluetooth Piconet 2
User C's PDA
User B's Mobile Phone
User B's PDA
Remote Laptop (Laptop E) is connected to Piconet 1 through router (Laptop D).
User C's Laptop Master of Piconet 3
User B's Laptop Master of Piconet 2
Laptop
User A's Laptop Master of Piconet 1
Laptop D
Laptop
Laptop E
Bluetooth Piconet 1
Scenario 1 (Piconet 1): Laptops of separate users in a meeting Sharing files and contact information (e.g., meeting attendee list).

- Eight devices can be connected in what is known as a Piconet. Only one of them acts as the master and the others are slaves.
- Two or more piconets can form a Scatternet via a bridge node.
- There can be 255 low power parked nodes, who can respond to the master only
- The Piconet is a TDM system with the master controlling the clock and decide which slave get the time slot
- Connection between master and slave only

Typical Bluetooth Network—A Scatternet

Characteristics of Bluetooth Technology



Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 – 2.4835 GHz (ISM band).
Hop Frequency	1,600 hops/sec.
Data Rate	1 Mbps (raw). Higher bit rates are anticipated.
Data and Network Security	Three modes of security (none, link-level, and service level), two levels of device trust, and three levels of service security. Stream encryption for confidentiality, challenge-response for authentication. PIN-derived keys and limited management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters.
Throughput	Up to approximately 720 kbps.
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a $5 cost projected. Low power and minimal hardware.
Negative Aspects	Possibility for interference with other ISM band technologies. Relatively low data rates. Signals leak outside desired boundaries.

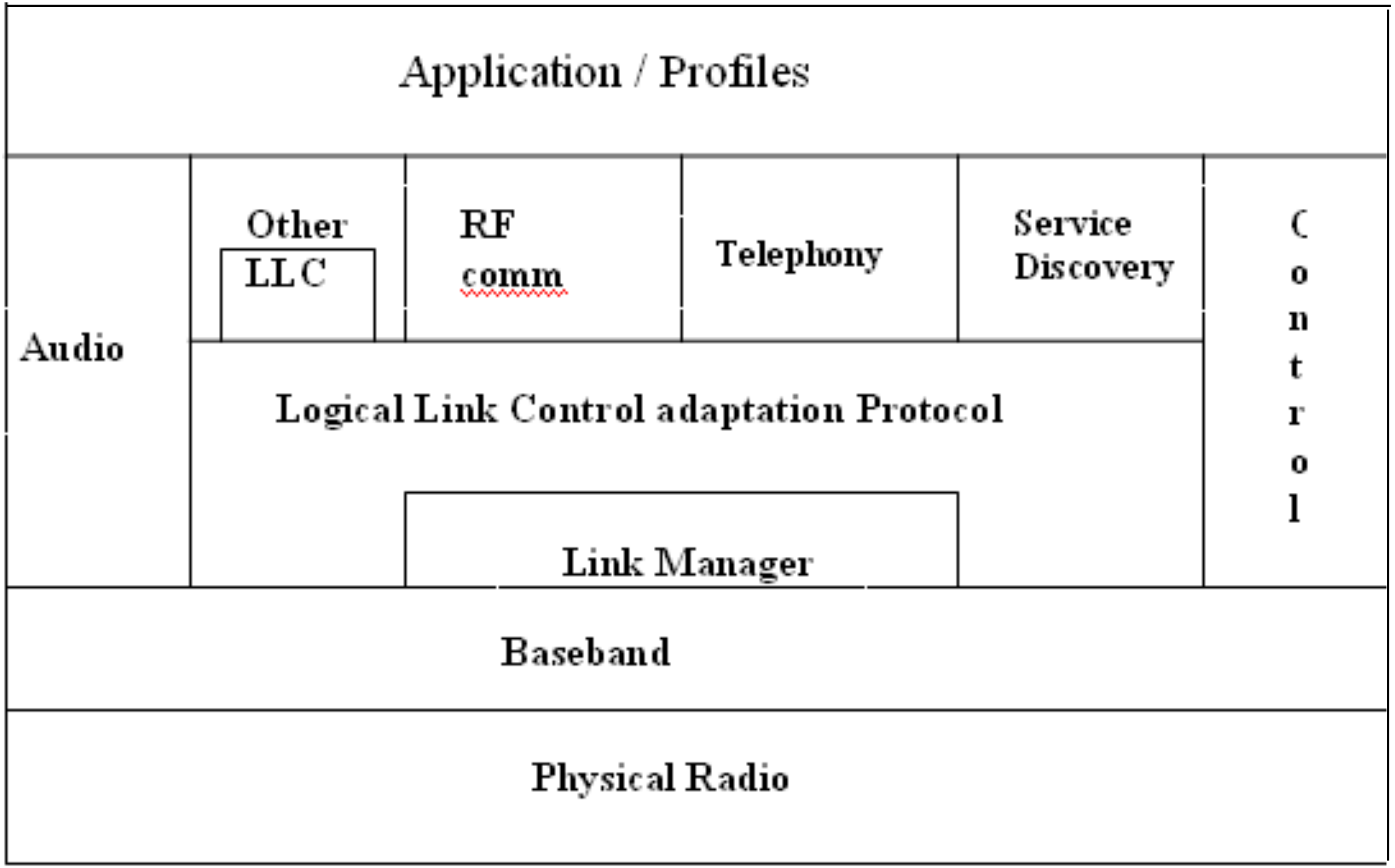
Benefits of Bluetooth:

- No cable connection
- Ease of file sharing
- Wireless synchronization
- Automated wireless applications
- Internet connectivity

Bluetooth Applications (profiles)

Name	**Description**
Generic access	procedures of secure link establishment and management
Service discovery	to discover what services other devices offer
Serial port	transport protocol for emulating a serial line
Generic object exchange	Defines a c-s relationship for data movement
LAN access	protocol between a mobile and a fixed LAN
Dial-up networking	allows a laptop to call via mobile phone
Fax	as above but to send faxes
Cordless telephony	to connect a handset and its local base station
Intercom	digital walkie-talkie between two telephones
Headset	allows hands-free voice communication (between headset and base station)
Object push	way to exchange simple objects
File transfer	more general file transfer facility
Synchronization	allows a PDA to synchronize with another computer

Bluetooth Protocol Stack



Application / Profiles

Audio

Other LLC

RF comm

Telephony

Service Discovery

Control

Logical Link Control adaptation Protocol

Link Manager

Baseband

Physical Radio

The Bluetooth Radio Layer

- It moves the bits from the master to the slave and vice versa with a range of 10m.
- Bluetooth transceivers uses Gaussian Frequency Shift Keying (GFSK) modulation.
- The theoretical maximum bandwidth of a Bluetooth network is 1 Mbps.
- The second generation of Bluetooth technology is expected to provide a maximum bandwidth of 2 Mbps.
- Bluetooth networks can support either one asynchronous data channel with up to three simultaneous synchronous speech channels or one channel that transfers asynchronous data and synchronous speech simultaneously.
- Bluetooth uses a combination of packet-switching technology and circuit-switching technology.

Bluetooth Baseband layer:

- Allows links to be established with other Bluetooth devices.
- It turns the raw bit stream into frames with 1, 3, or 5 slots in length.
- Each frame is transmitted on a logical channel, called link, between the master and a slave.
- Master provides 625 μs TDM time slot
- Master transmits in the even slots, all the slaves transmit in odd slots
- Two kinds of links are there:
  - ACL (Asynchronous connection-less) used for packet switched data transfer with L2CAP. A slave may have one ACL link with the master
  - SCO (synchronous connection-oriented) links for real time data like telephony

Link Manager Protocol (LMP)

- It communicates with its peer in the target device. It defines the messages used by software in the master for polling the client even when the master has no data to transport. LMP messages are transported in the payload data field of a Bluetooth data packet.
- These messages also control authentication and encryption.

Logical Link Control and Adaptation Protocol (L2CAP):

- Adapter between upper and lower layer
- Used by upper layer protocols for data transport.
- Provides both connection-less and connection-oriented service.
- L2CAP is responsible for upper level protocol data segmentation and reassembly as well as transport of quality of service information.
- Accepts blocks of data up to 64 kB in length and will reliably transport them to its peer in the target device.

Bluetooth Audio Protocol:

- Belongs to the data link level
- Use the SCO (synchronous connection orientated) link for synchronous communication. An application can obtain synchronous services simply be opening a voice data link.

Service Discovery Protocol (SDP) is used to find new services as they become available and to deregister services that become unavailable. It is optimized for a fast changing environment.

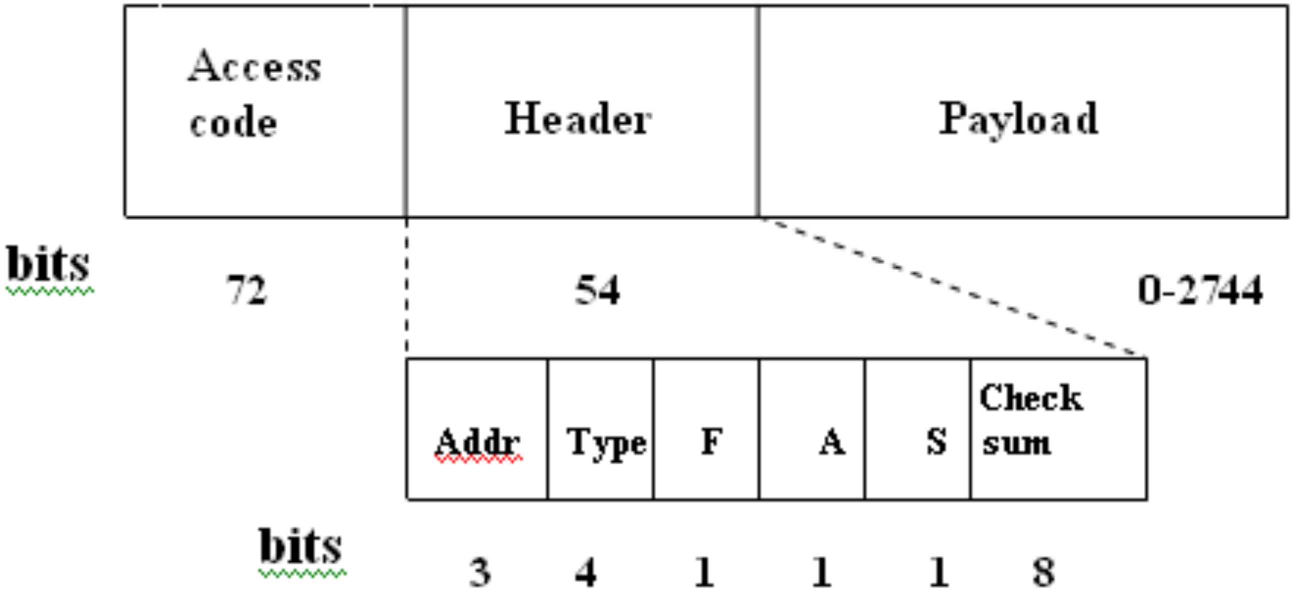
Bluetooth Tracking Services

— A Piconet is formed in an ad hoc manner when the devices come in proximity

— All Bluetooth devices include an SDP server application that keeps track of the services available on every device.

- **Radio frequency Communication Interface (RFCOMM)** provides an RS-232 serial port emulation to the application or to higher level protocols.
- **Bluetooth Telephony Control Protocol Specification – Binary (TCS-BIN)** defines the necessary call control signaling for establishing a voice connection between Bluetooth devices. It has three major components.
  - Call control component
  - Group management
  - Connection-less TCS component
- **Advanced Telephony (AT)** commands enable telephony control.
- The IP stack can be used to provide Wireless Access Protocol (WAP) capability on Bluetooth devices. WAP provides services such as email delivery across wireless links.
- **Object Exchange Protocol (OBEX),** which is used to exchange data objects. OBEX provides a session layer service for applications such as synchronization and file transfer.

Bluetooth Frame Structure



Access code	Identifies the master
AM_ADDR	3-bit active member address to distinguish active members in a piconet
TYPE	4-bit type code to distinguish between 16 different types of packets, ACL, SCO, poll, null type
FLOW	1-bit flow control over ACL link, asserted by the slave when its buffer is full
ARQN	1-bit acknowledgement indication of success of transfer of the packet
SEQN	SEQN bit provides a sequential numbering scheme to order the data packet stream, helps in retransmission
HEC	8-bit checksum, header error check to check the header integrity

Questions?