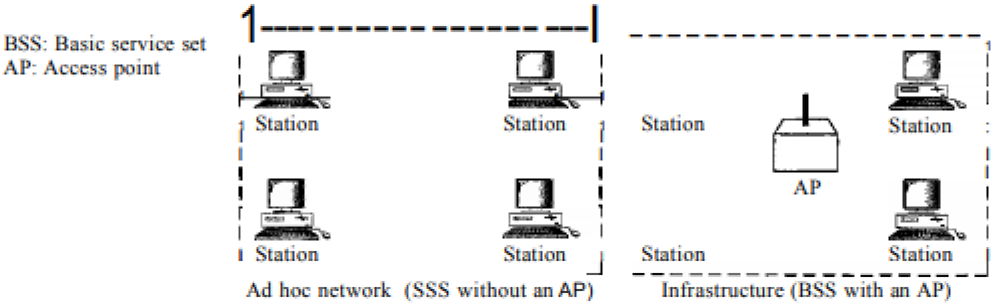
IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Architecture

- The standard defines two kinds of services:
    - the basic service set (BSS)
    - Extended service set (ESS).
- **Basic Service Set**
    - IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).
    - Figure 14.1 shows two sets in this standard.
        - **Adhoc** -A BSS without an AP is called an ad hoc network.
        - **Infrastructur**e- BSS with an AP is called an infrastructure network

Figure 14.1 *Basic service sets (BSSs)*



Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs.

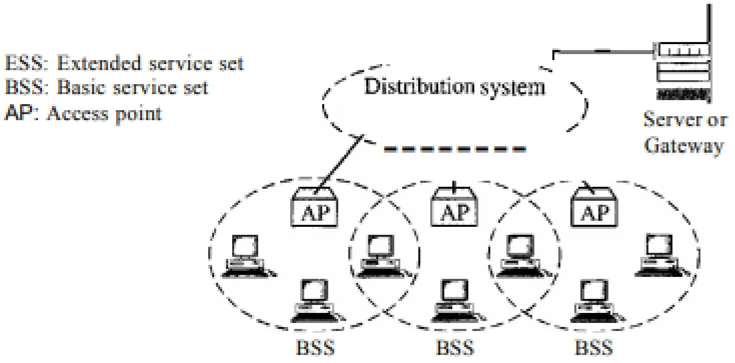
In this case, the BSSs are connected through a **distribution system**, which is usually a wired LAN. The distribution system connects the APs in the BSSs.

The extended service set uses two types of stations:

- **Mobile**- normal stations inside a BSS
- **Stationary** -. AP stations that are part of a wired LAN The mobile stations are. The stationary stations are.

Figure 14.2 shows an ESS.

Figure 14.2 *Extended service sets (ESSs)*

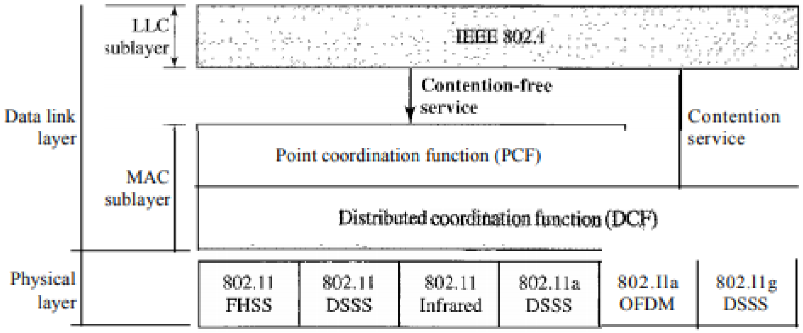


Station Types

- IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:
  - no-transition- mobility is either stationary (not moving) or moving only inside a BSS
  - BSS·transition- transition mobility can move from one BSS to another, but the movement is confined inside one ESS
  - ESS-transition mobility-can move from one ESS to another

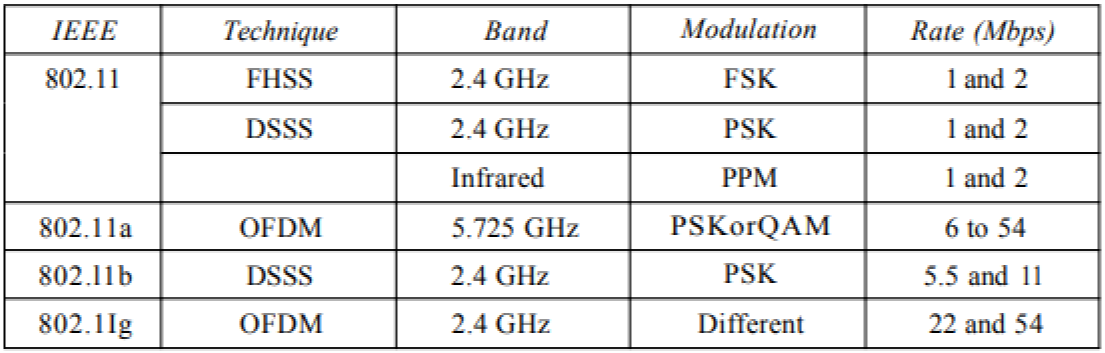
Physical Layer

Figure 14.3 *MAC layers in IEEE 802.11 standard*



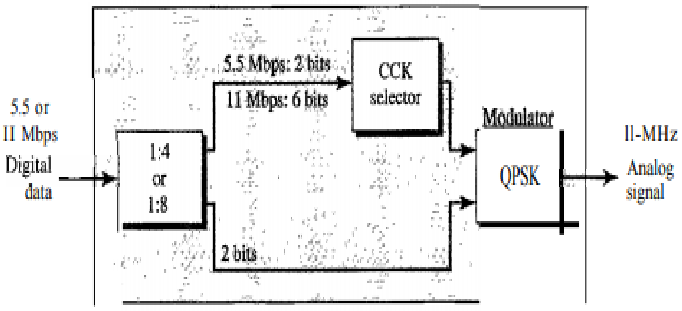
Physical Layer

Table 14.4 *Physical layers*



IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSKorQAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.1lg	OFDM	2.4 GHz	Different	22 and 54

INFRARED	Applicable for 1-2 Mbps. Not very popular, also because sunlight degrades performance
IEEE 802.11 FHSS Frequency Hopping Spread Spectrum	Use 79 channels, each 1 MHz wide in an unregistered band (i.e., free to be used) frames are sent at different frequencies each time low bandwidth, but good resistance against security attacks and interference from other devices.
IEEE 802.11 DSSS Direct Sequencing Spread Spectrum	Similar to CDMA, restricted to 1-2 Mbps
IEEE 802.lla OFDM Orthogonal FDM	Akin to ADSL: apply FDM across multiple channels (48 for data, 4 for control). Can reach 54 Mbps All the subbands are used by one source at a given time. Sources contend with one another at the data link layer for access. The band is divided into 52 subbands, with 48 subbands for sending 48 groups of bits at a time and 4 subbands for control information. Dividing the band into

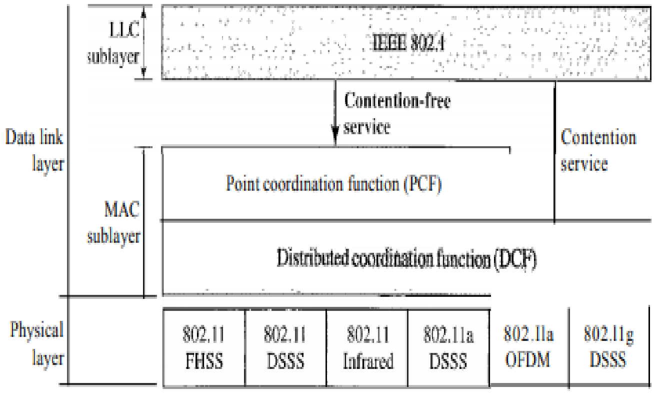
	subbands diminishes the effects of interference. If the subbands are used randomly, security can also be increased.
IEEE (802.11b) High Rate Direct Sequencing	Akin to DSS - use 11 million chip sequences to get to 11 Mbps Encoding method CCK-Complementary code keying. To be backward compatible with DSSS, HR-DSSS defines four data rates: 1 2 5.5 11 Mbps. The first two use the **same modulation techniques** as DSSS. The 5.5-Mbps version uses **BPSK** and transmits at 1.375 Mbaudls with **4-bit CCK** encoding. The II-Mbps version uses **QPSK** and transmits at 1.375 Mbps with **8-bit** CCK encoding. Figure Figure 14.18 *Physical layer ofIEEE 802.11b*  5.5 or II Mbps Digital data 1:4 or 1:8 5.5 Mbps: 2 bits 11 Mbps: 6 bits CCK selector 2 bits Modulator QPSK II-MHz Analog signal
IEEE 802.11n	a proposed amendment to the IEEE 802.11 standard to significantly improve network throughput .It leverages off Space Division Multiplexing (SDM) improves performance by

	parsing data into multiple streams transmitted through multiple antennas (up to four) Multiple-input and multiple-output (MIMO) it also increase power consumption and cost In addition the bandwidth of each channel is moved to 40 Mhz (instead of the standard 20 Mhz) total throughput per channel is 150 Mb Combining four 40 Mhz channels with MIMO we get a data rate of 600 Mbps in practice, speeds of 100Mbit/sec. to 140Mbit/sec. 'MIMO-based' products (e.g., NETGEAR or Apple)

MAC Sublayer

- IEEE 802.11 defines two MAC sublayers: the ***distributed coordination function (DCF) and point coordination function (PCF).***
-

Figure 14.3 *MAC layers in IEEE 802.11 standard*



-

DCF(***distributed coordination function)***

DCF uses CSMA/CD

- CSMA/CD

- It has two methods operations:
  - Ethernet-like
  - MACAW

Ethernet-Persistent Strategy

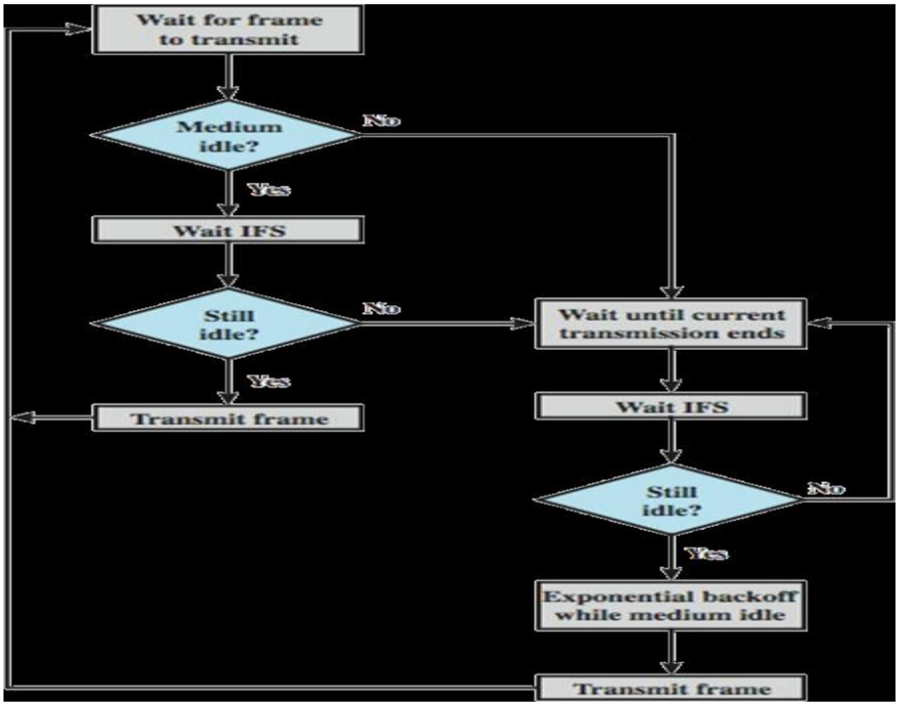
Step 1. When a station wants to transmit, it senses the channel

Step 2. If it is idle,wait for a fixed interval (IFS) and then transmits

Step 3. Otherwise, it waits until the transmission ends,then wait for another IFS and finally wait for a random time before transmitting

- exponential backoff is used

Step 4. if a collision occurs (i.e., no ack received), the process restarts


Wait for frame to transmit
Medium idle?
No
Yes
Wait IFS
Still idle?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle?
No
Yes
Exponential backoff while medium idle
Transmit frame

MACAW

1. Before sending a frame, the source station senses the medium by checking the energy level at the carrier frequency

a. The channel uses a persistence strategy with back-off until the channel is idle.

b. After the station is found to be idle, the station waits for a period of time called the distributed interframe space (DIFS); then the station sends a control frame called ***the request to send*** (RTS).

2. After receiving the RTS and waiting a period of time called the short interface space (SIFS), the destination station sends a control frame, called the ***clear to send (CTS)***, to the source station. This control frame indicates that the destination station is ready to receive data.

3. The source station sends data after waiting an amount of time equal to SIFS. 4. The destination station, after waiting an amount of time equal to SIFS, sends an acknowledgment to show that the frame has been received. Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination

Network allocation vector (NAV)

- When a station sends an RTS frame, it includes the duration of time that it needs to occupy the channel.
- The stations that are affected by this transmission create a timer called a network allocation vector (NAV) that shows how much time must pass before these stations are allowed to check the channel for idleness. Each time a station accesses the system and sends an RTS frame, other stations start their NAV

Point coordination function

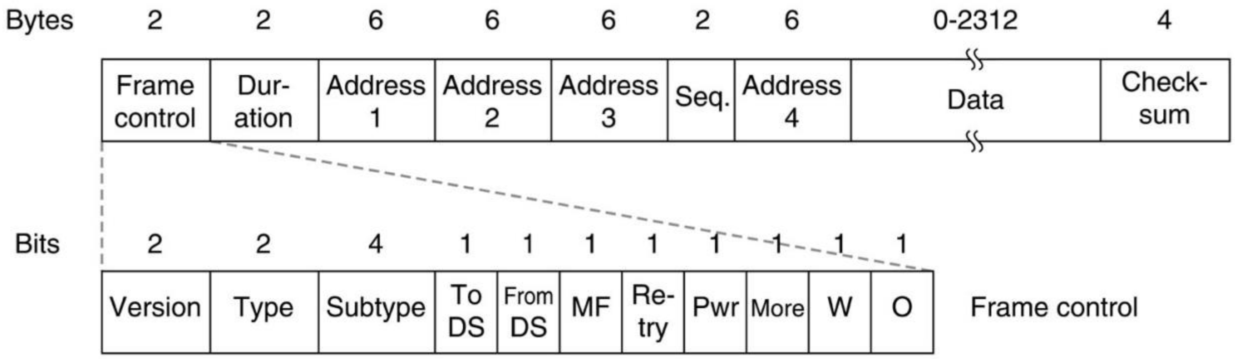
- *Implemented in an infrastructure network.*
- In PCF the base-station polls the other stations, asking them if they have anything to send
- It sends a ***beacon frame*** once every 10 or 100 ms. This frame carries information on frequencies and such, and invites stations to sign up for transmission. To save battery, a base station can also direct a mobile station to go into ***sleep*** state incoming

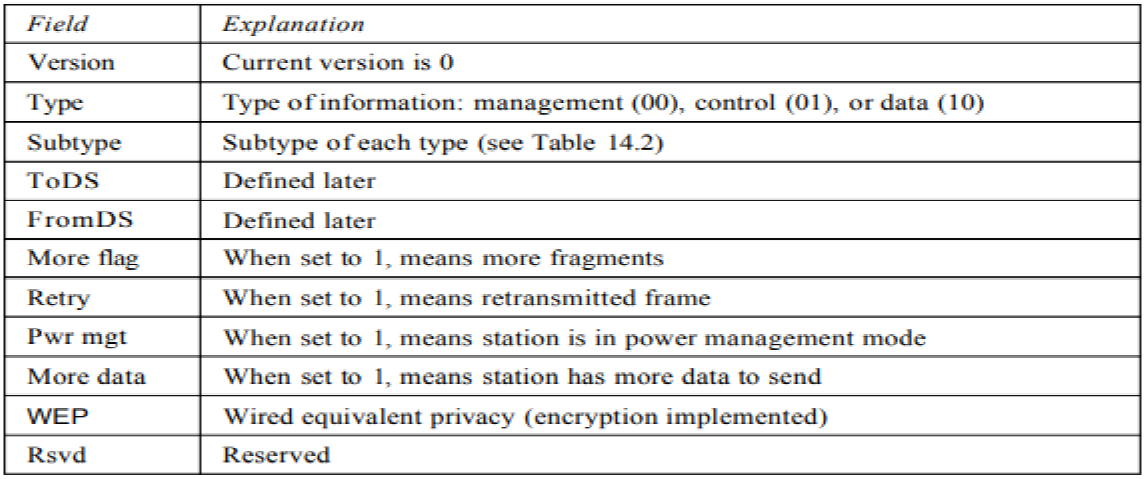
messages will be buffered until it wakes up .When base station transmits, there can be no hidden terminals.

Fragmentation

The wireless environment is very noisy; a corrupt frame has to be retransmitted. The protocol, therefore, recommends fragmentation-the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.

Frame Format





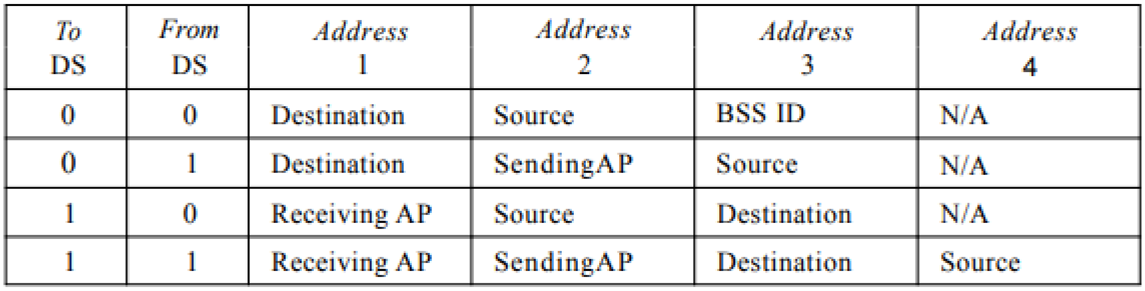
Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 14.2)
ToDS	Defined later
FromDS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

DS: Is the frame entering/leaving the current cell?

MF: Frames are allowed to be fragmented to increase reliability.This bit tells whether more fragments are on their way.

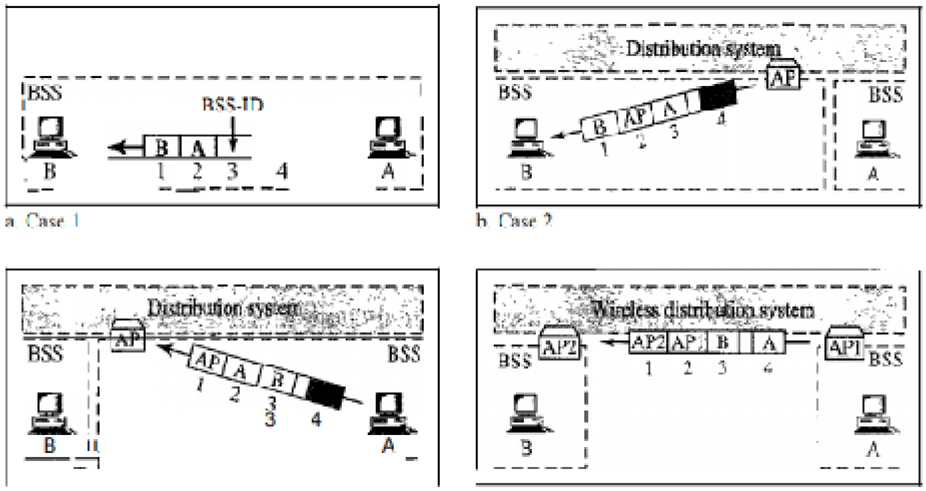
Duration: Tells how long the transmission of this frame will take,allowing other stations to set their NAV accordingly.

Addresses: Source/destination in a cell; and those of base stations outside the cell when dealing with intercell traffic.



To DS	*From* DS	*Address* 1	*Address* 2	*Address* 3	*Address* 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	SendingAP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	SendingAP	Destination	Source

Figure 14.9 *Addressing mechanisms*



a. Case 1

b. Case 2

c. Case 3

d. Case 4

(i) Case 2: 01 In this case, To DS = 0 and From DS = 1. This means that the frame is

Sequence: Sequence number of this frame. 4 bits are used to identify a fragment of a frame.

Frame body. This field, which can be between 0 and 2312 bytes, contains information based on the type and the subtype defined in the FC field.

FCS. The FCS field is 4 bytes long and contains a CRC-32 error detection sequence.

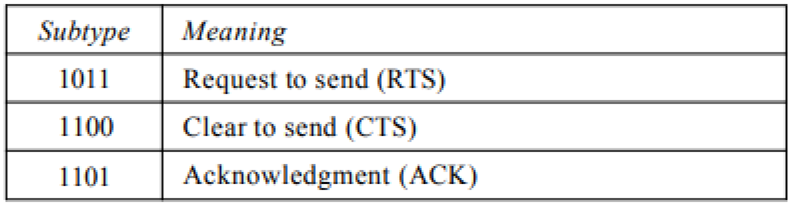
FRAME TYPES

3TYPES

(1)Management Frames – used for initial communication between station and access point.

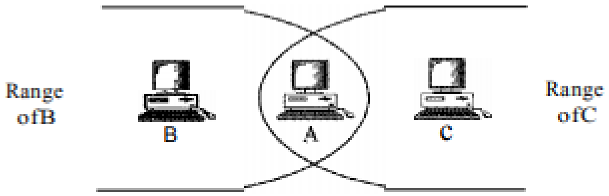
(2)Control Frames –used for accessing the channel and acknowledging frames

(3)**Data frames** - used for carrying data and control information.



Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

Hidden Station Problem

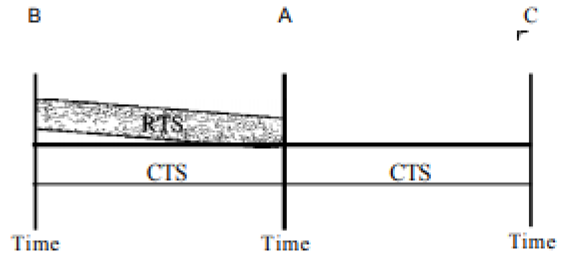


Band Care hiddent from each other with respect to A.

- Assume that station B is sending data to station A. In the middle of this transmission, station C also has data to send to station A. However, station C is out of B's range and transmissions from B cannot reach C. Therefore C thinks the medium is free. Station C sends its data to A, which results in a collision at A because this station is receiving data from both B and C. In this case, we say that stations Band C are hidden from each other with respect to A. Hidden stations can reduce the capacity of the network because of the possibility of collision.
- **Solution** to the hidden station problem is the use of the handshake frames (RTS and CTS).

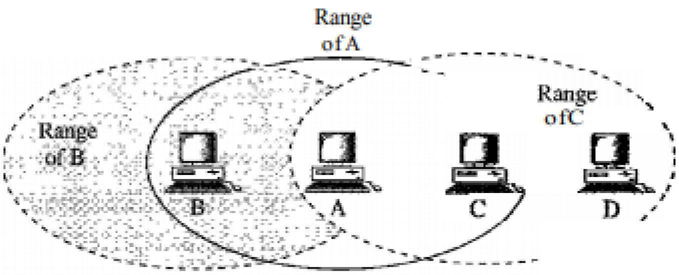
  shows that the RTS message from B reaches A, but not C. However, because both Band C are within the range of A, the CTS message, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel and refrains from transmitting until that duration is over.

Use ofhandshaking to prevent hidden station problem



Exposed station problem

Exposed station problem



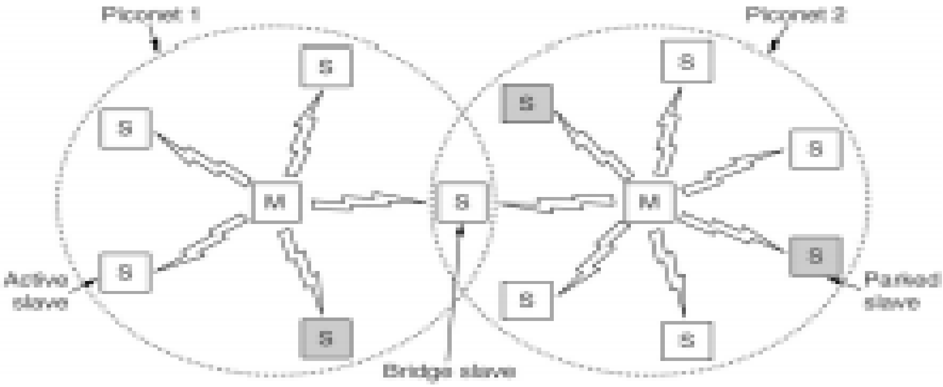
C is exposed to transmission from A to B.

In Figure 14.12, station A is transmitting to station B. Station C has some data to send to station D, which can be sent without interfering with the transmission from A to B. However, station C is exposed to transmission from A; it hears what A is sending and thus refrains from sending. In other words, C is too conservative and wastes the capacity of the channel.

Bluetooh (802.15)

- Bluetooth is to allow very different (portable and fixed) devices located in each other's proximity to exchange information:
    - Let very different portable devices (PDA, cellular phone, notebook) set up connections
    - Replace many of the existing cables (headset, keyboard, mouse, printer)
    - Provide better wireless connection (handsfree solutions)
    - Provide wireless access to Internet entry points
    - Relatively high bandwidth: 1 Mbit/second Also referred to as IEEE 802.15.1 It's named after a Viking king who unified Denmark and Norway (940-981)

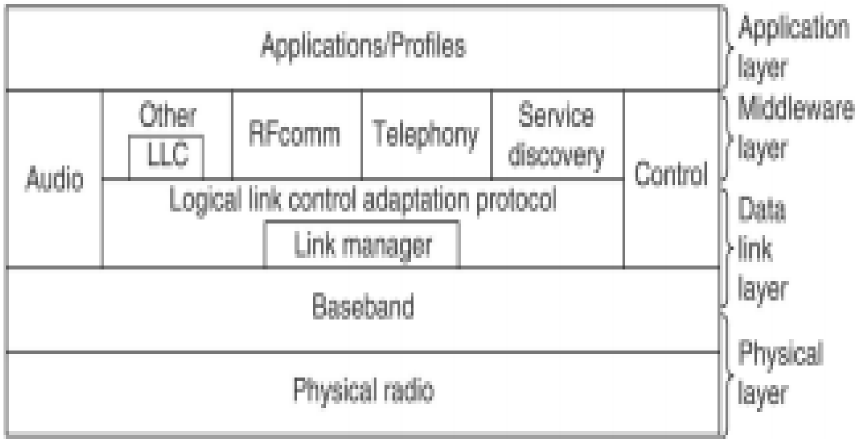
Bluetooth Architecture



- **Piconet**:
    - Group of devices with one master and multiple slaves. there can as much as 7 active slaves, but a total of 255 parked ones (i.e., in a power-saving state).
- **Scatternet**:
    - An interconnected collection of piconets.

A piconet is a centralized TDM system with the master determining which device gets to communicate the connection procedure and for a non-existent piconet connection procedure is initiated by any of the devices, which then becomes the master.

BLUETOOTH PROTOCOL STACK



Radio:

- it uses frequency hopping spread spectrum-FHSS***(2.4 GHz band***)
- Divided into 79 channels
- take data signal and modulate it with a carrier signal that changes frequency in hops.
    - good to minimize interference from other devices (microwave ovens!)
- hops for Bluetooth: fixed at fc=2402 + k MHz, k = 0, 1, . . . , 78.
- **modulation** is ***frequency shift keying*** with 1 bit / Hertz ⇒ 1Mbps data rate but much of this is consumed as overhead

Baseband: Core of the data link layer. –access method is **TDMA(half duplex)**

- determines timing, framing, packets, and flow control.
- provides synchronous and asynchronous data communication.
- error correction can be used to provide higher reliability

Link manager:

- Manages connections, power management

Logical link control:

- Multiplexing of higher-level protocols, segmentation and reassembly of large packets, device discovery

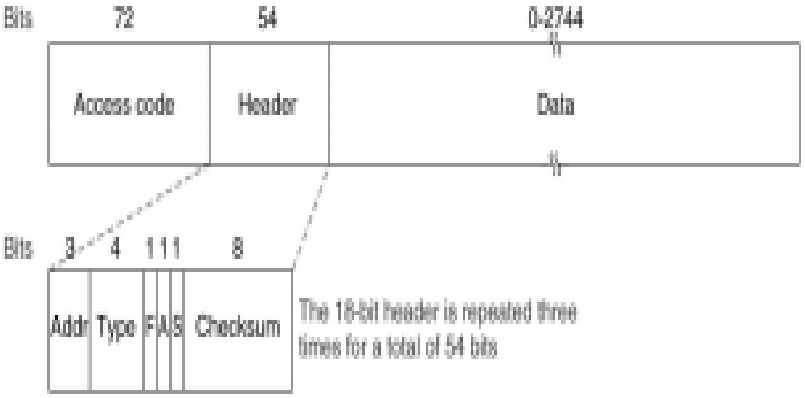
Audio:

- Handles streaming for voice-related applications

RFCOMM:

- Emulate serial cable based on GSM protocol

BLUETOOTH FRAME STRUCTURE



- **Access code** identifies the master of the piconet slaves within radio range of two masters do not interfere
- **Address** identifies the recipient among the eight active devices
- The **Flow bit** is asserted by a slave when its buffer is full and cannot receive any more data
- The **Acknowledgment bit** is used to piggyback an ACK The Sequence bit is used to number the frame.
    - Stop-and-wait protocol is used so 1 bit is enough
- The **18-bit header** is repeated three times (54-bit header)
    - On the receiving side, all three copies are examined.
    - if all three are the same, the bit is accepted.

  - if not, the majority opinion wins

Two types of links

Two types of links can be created between a primary and a secondary:

SCQ links - A synchronous connection-oriented (SeQ) link is used when avoiding latency (delay in data delivery) is more important than integrity (error-free delivery).

ACL links. - An asynchronous connectionless link (ACL) is used when data integrity is more important than avoiding latency

L2CAP(Logical Link Control and Adaptation Protocol)

Used to exchange data on ACL link

Format of data packet

Length(2 bytes)	Channel ID(2 bytes)

The I6-bit length field defines the size of the data, in bytes, coming from the upper layers. Data can be up to 65,535 bytes. The channel ID (CID) defines a unique identifier for the virtual channel created at this level (see below). The L2C

The L2CAP has specific duties:

- multiplexing,
- segmentation and reassembly,
- quality of service (QoS), and
- group management.

PPP(Point to point protocol)

PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

• This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

1.Defines the format of the frame

2. It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

3. It defines how network layer data are encapsulated in data link frame.

4. PPP provides error detection.

5. Unlike SLIP that supports only IP, PPP supports multiple protocols.

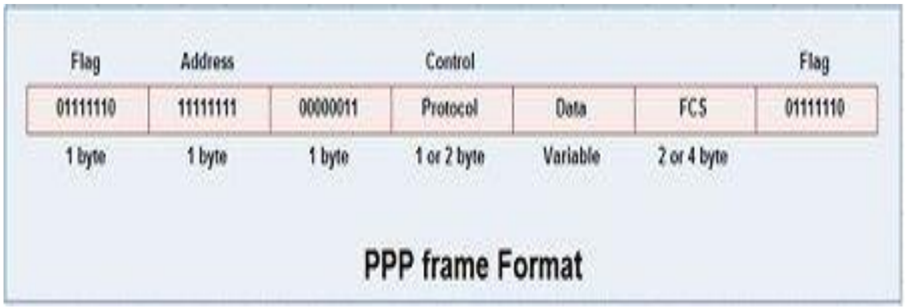
6. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



Flag	Address		Control			Flag
01111110	11111111	00000011	Protocol	Data	FCS	01111110
1 byte	1 byte	1 byte	1 or 2 byte	Variable	2 or 4 byte	

PPP frame Format

1. **Flag field**: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

2. **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

3. **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the

frame does not contain any sequence numbers and there is no flow control or error control.

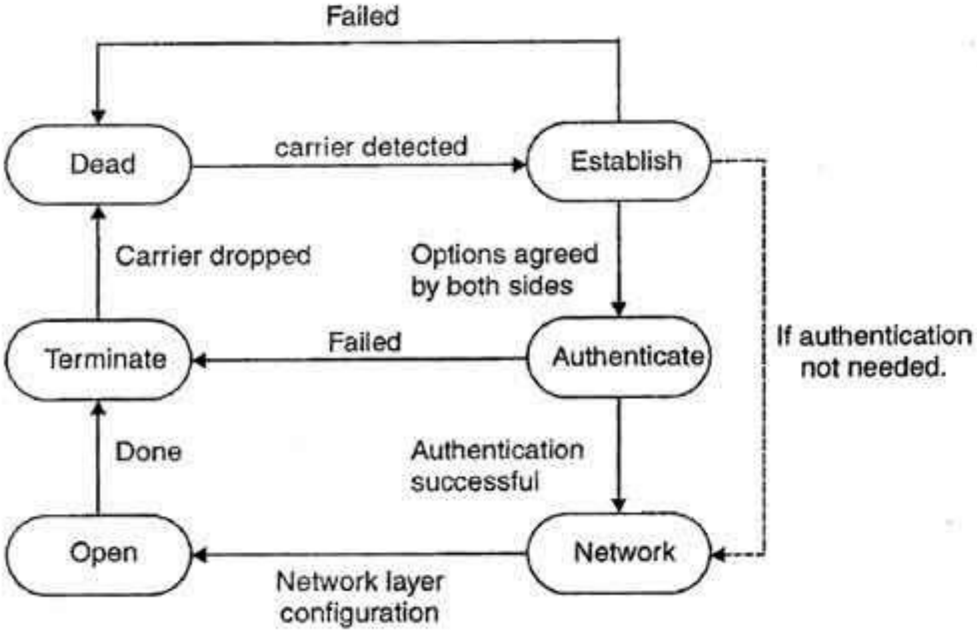
4. **Protocol field**: This field specifies the kind of packet in the data field *i.e*. what is being carried in data field.

5. **Data field**: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

6. **FCS field**: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Transition Phases in PPP

- The PPP connection goes through different states as shown in fig.
  - **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.


Failed
Dead
carrier detected
Establish
Carrier dropped
Options agreed by both sides
Terminate
Failed
Authenticate
If authentication not needed.
Done
Authentication successful
Open
Network
Network layer configuration

Transition phases

  - **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

  - **Authenticate**: This phase is optional. The two nodes may decide during the establishment phase, not to skip this phase. However if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

- **Network**: In network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

- **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

- **Terminate**: In this phase connection is terminated.

Point-to-point protocol Stack

PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.

The various protocols used are:

1. Link Control Protocol

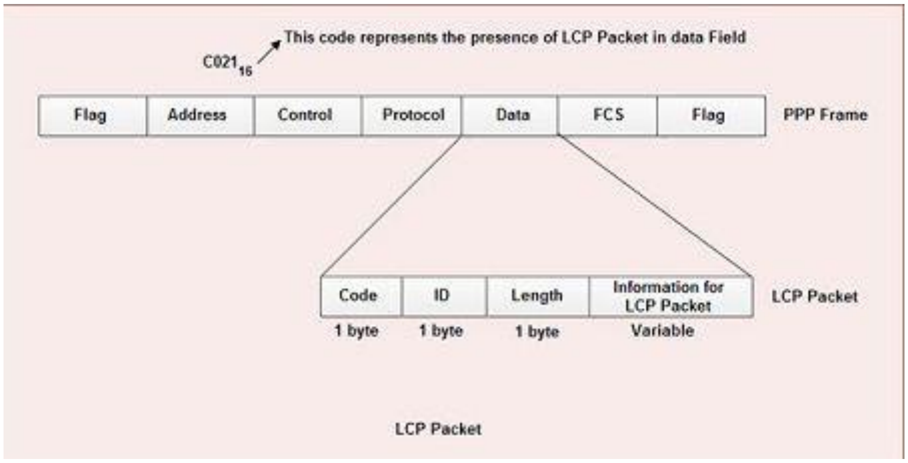
2. Authentication Protocol

3. Network Control Protocol

1. Link Control Protocol

• It is responsible for establishing, maintaining, configuring and terminating the link.

• It provides negotiation mechanism to set options between two endpoints.



LCP Packet

• All LCP packets are carried in the data field of the PPP frame.

• The presence of a value $C021_{16}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.

• The various fields present in LCP packet are:

1. **Code**: 1 byte-specifies the type of LCP packet.

2. **ID**: 1 byte-holds a value used to match a request with the reply.

3. **Length**: 2 byte-specifies the length of entire LCP packet.

4. **Information**: Contains extra information required for some LCP packet.

• There are eleven different type of LCP packets. These are categorized in three groups:

1. **Configuration packet**: These are used to negotiate options between the two ends. For example: configure-request, configure-ack, configure-nak, configure-reject are some configuration packets.

2. **Link termination packets**: These are used to disconnect the link between two end points. For example: terminate-request, terminate-ack, are some link termination packets.

3. **Link monitoring and debugging packets**: These are used to monitor and debug the links. For example: code-reject, protocol-reject, echo-request, echo-reply and discard-request are some link monitoring and debugging packets.

2. Authentication Protocol

Authentication protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

1. Password Authentication Protocols (PAP)

2. Challenge Handshake Authentication Protocol (CHAP)

4 types of CHAP packets:

1. Challenge-used by system to send challenge value.

2. Response-used by the user to return the result of the calculation.

3. Success-used by system to allow access to the system.

4. Failure-used by the system to deny access to the system.

3. Network Control Protocol (NCP)

• After establishing the link and authenticating the user, PPP connects to the network layer. This connection is established by NCP.

• Therefore NCP is a set of control protocols that allow the encapsulation of the data coming from network layer.

• After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.