Bluetooth - 1

- Bluetooth Architecture (WS:15.1 + PK:13.4)
- Protocol Architecture (WS:15.1 + PK:13.4)
- Radio Specification (WS:15.2 + PK:13.4)
- Baseband Specification (WS:15.3 + PK:13.4)

Review

- The drive for IEEE802.11ax
- The maximum data rate in IEEE802.11ax
- The new technologies in IEEE802.11ax

Overview

- Bluetooth is an open specification for short-range wireless voice and data communications.
  - At 2.4 GHz IMS band
- Bluetooth – also the nickname of Harald Blaatand (Jelling, AD 940-981), King of Denmark and Norway.

Originated by Ericsson in 1994. Bluetooth SIG formed in 1998

Also, in IEEE 802.15.1 – part of WPAN

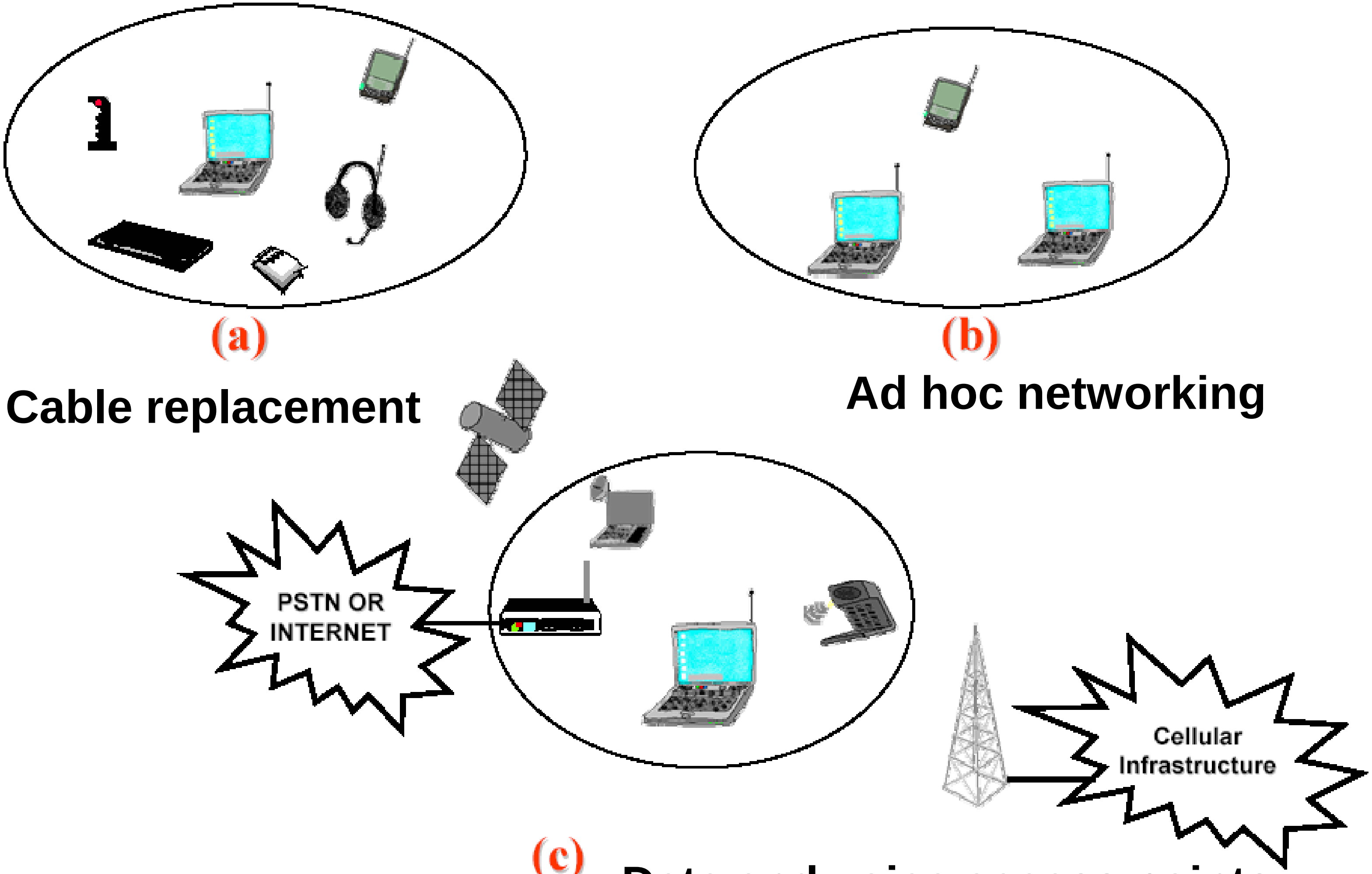
Bluetooth SIG -- more

- **February 1998: The Bluetooth SIG (IEEE802.15.1) is formed**
  - **promoter company group: Ericsson, IBM, Intel, Nokia, Toshiba**
- **May 1998: The Bluetooth SIG goes “public”**
- **July 1999: 1.0A spec (>1,500 pages) is published**
- **December 1999: ver. 1.0B is released**
- **December 1999: The promoter group increases to 9**
  - **3Com, Lucent, Microsoft, Motorola**
- **February 2000: There are 1,500+ adopters**
  - **adopters "enjoy" royalty free use of the Bluetooth technology**
    - **» products must pass Bluetooth certification**

The Bluetooth program overview

Bluetooth Promise	Wireless Connections Made Easy
Bluetooth Values	Freedom, Simplicity, Reliability, Versatility and Security
Usage Scenarios	What the technology can do
Specification Profiles	How to implement the usage scenarios
Certification Testing Interoperability	License free IP for adopters: product testing to ensure interoperability; protect the Bluetooth brand

Bluetooth Application Areas

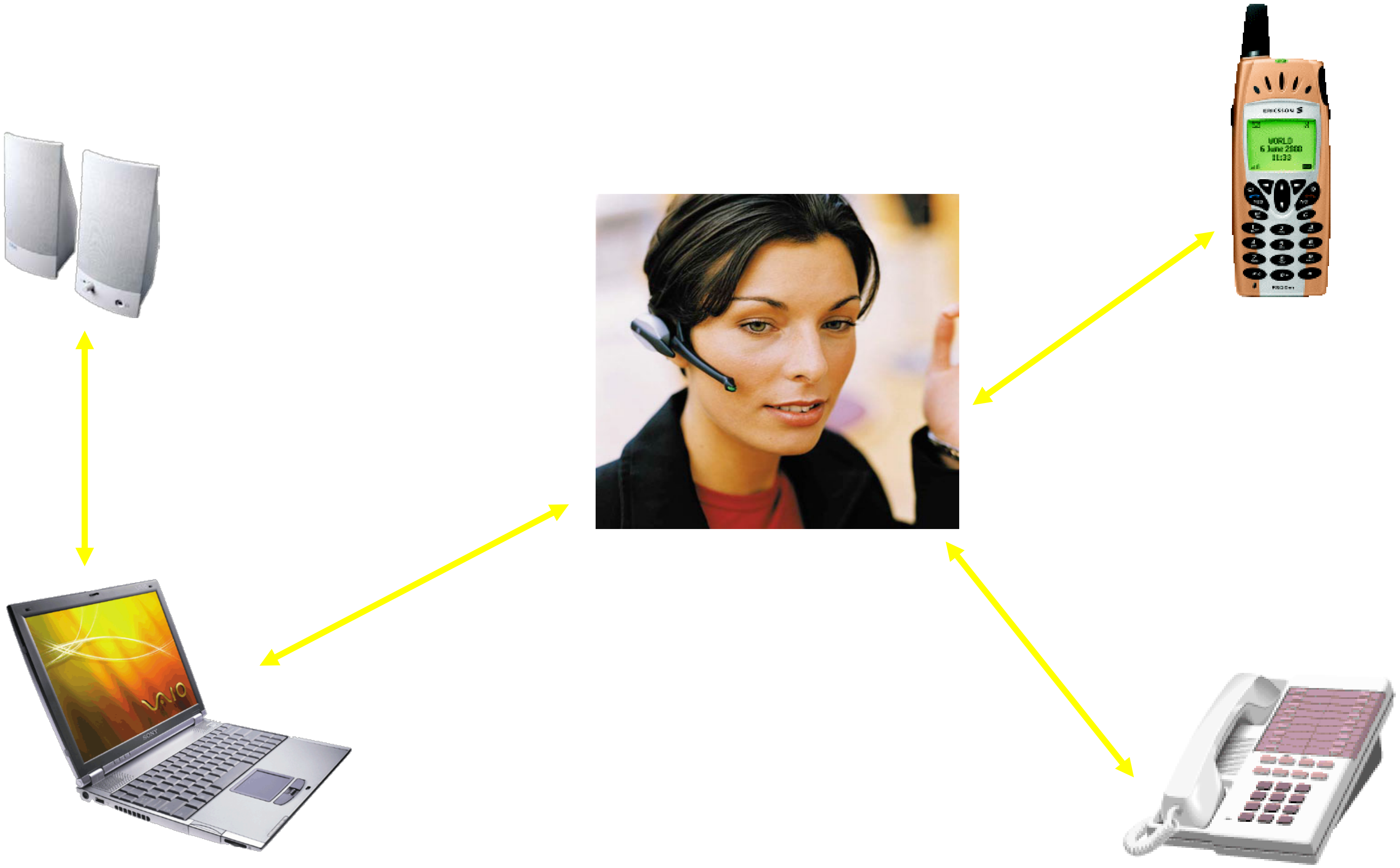


(a) Cable replacement

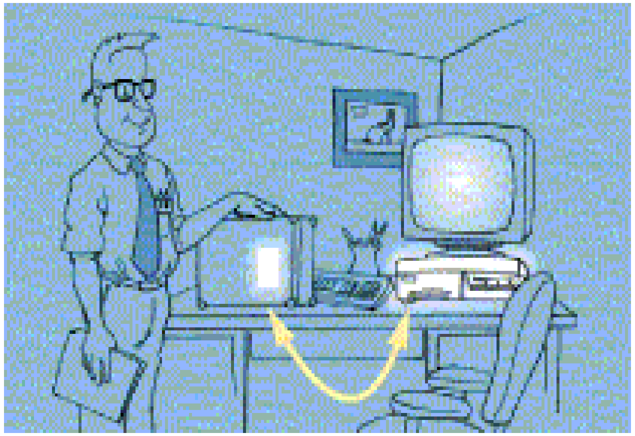
(b) Ad hoc networking

(c) Data and voice access points

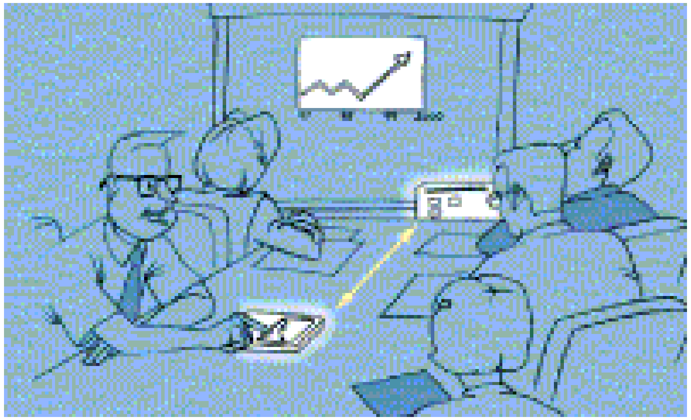
Ultimate Headset

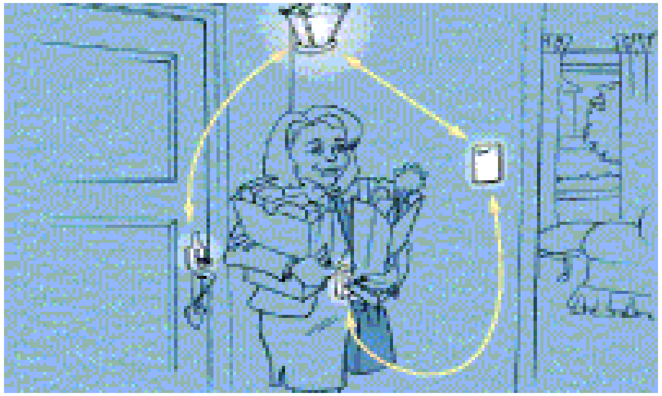


Automatic Synchronization

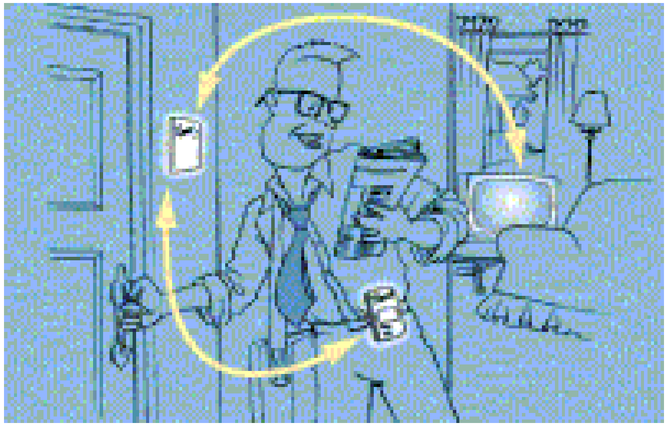


In the Office





At Home



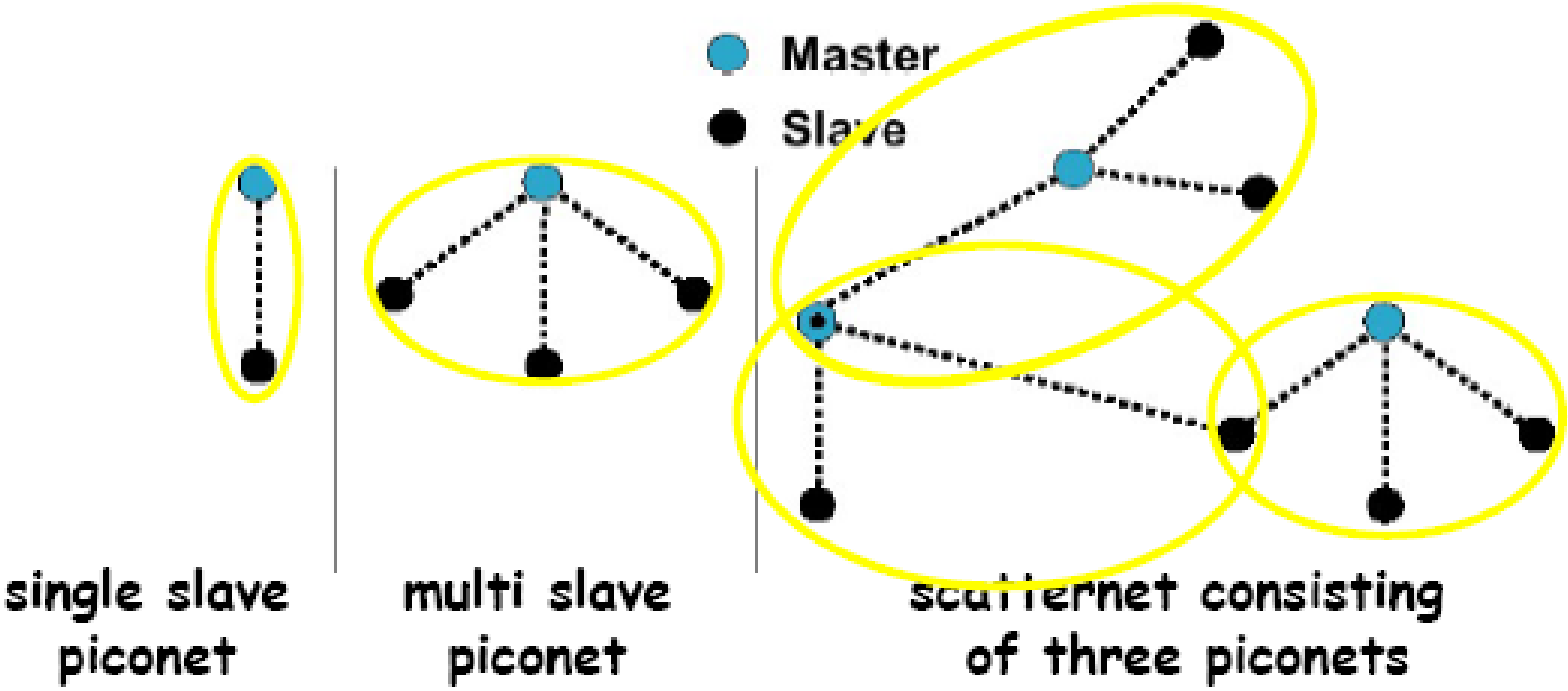
General Description

- A cable replacement technology
- Operates in the unlicensed ISM band at 2.4 GHz
- Frequency Hopping scheme (1600 hops/sec)
- 1 Mb/s symbol rate
- Range 10+ meters
- Single chip radio + baseband
- Key features:
  - » Robustness
  - » low complexity
  - » low power, and
  - » low cost.

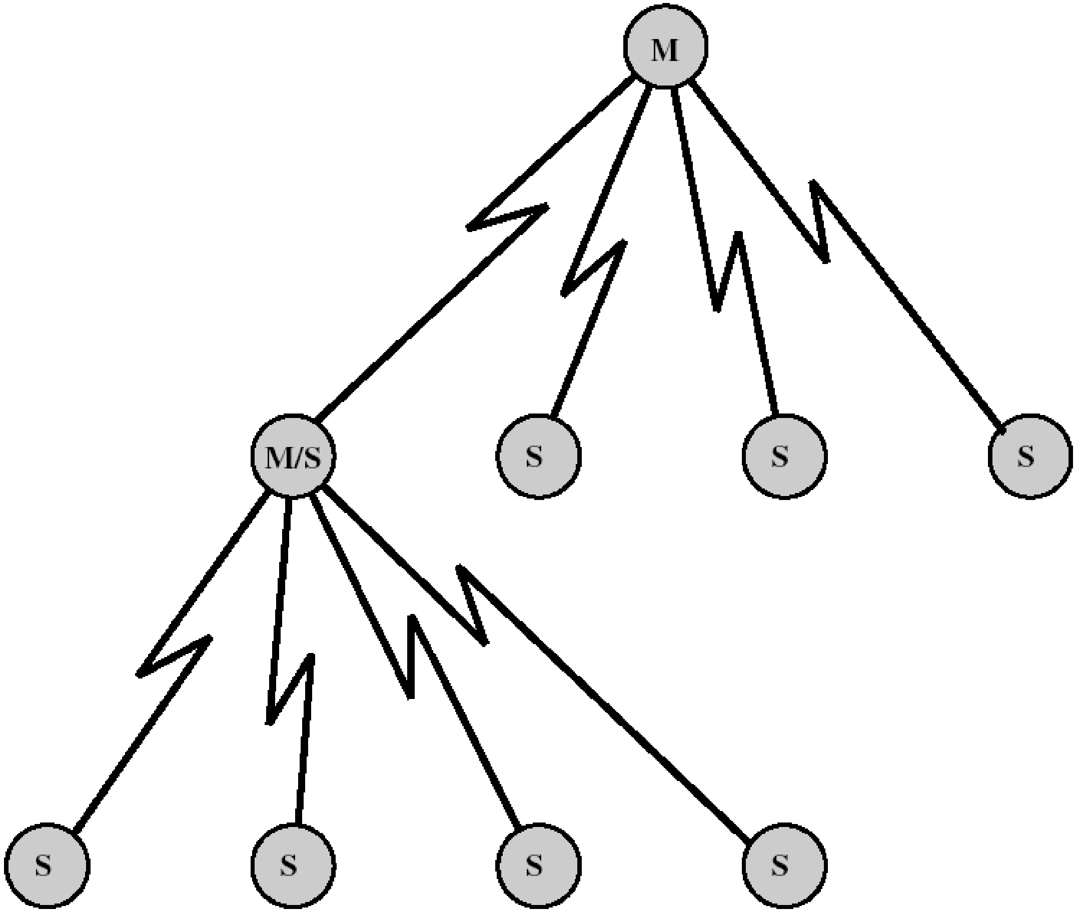
General Description (2)

- Bluetooth supports
  - Synchronous & asynchronous data channels.
    - » Three simultaneous synchronous voice channels, or
    - » One channel, with asynchronous data and synchronous voice
      - Each voice channel supports 64 kb/s in each direction.
  - The channel can support maximal 723.2 kb/s asymmetric (and still up to 57.6 kb/s in the return direction), or 433.9 kb/s symmetric.
- Bluetooth provides
  - point-to-point connection (only two BlueTooth units involved), or
  - point-to-multipoint connection.

Network Topology of Bluetooth

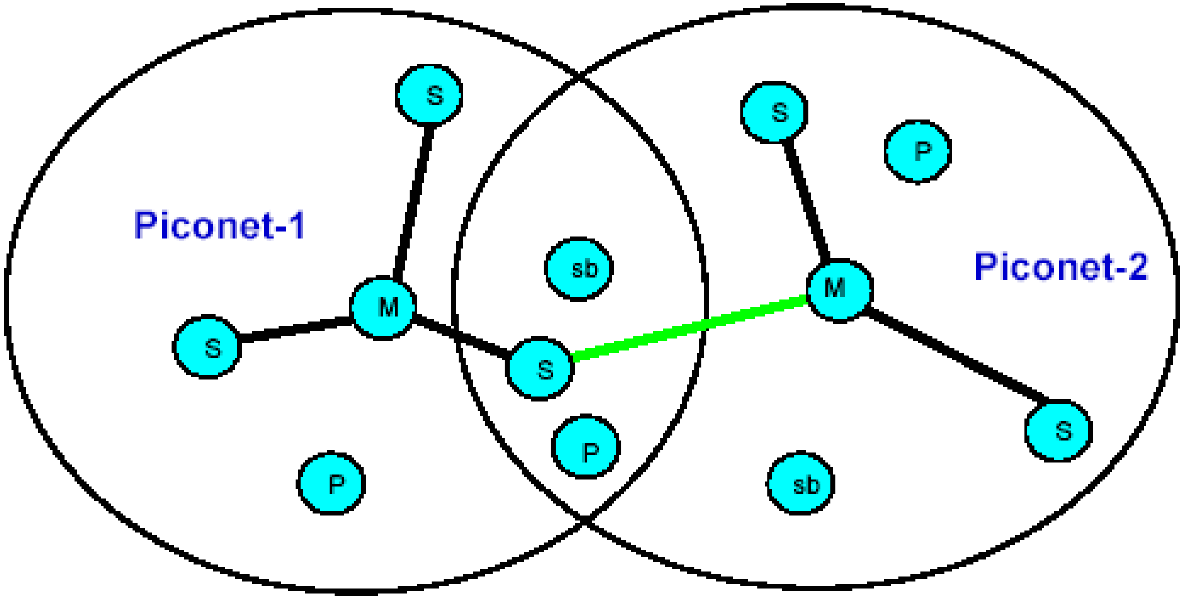


Piconet/Scatternet



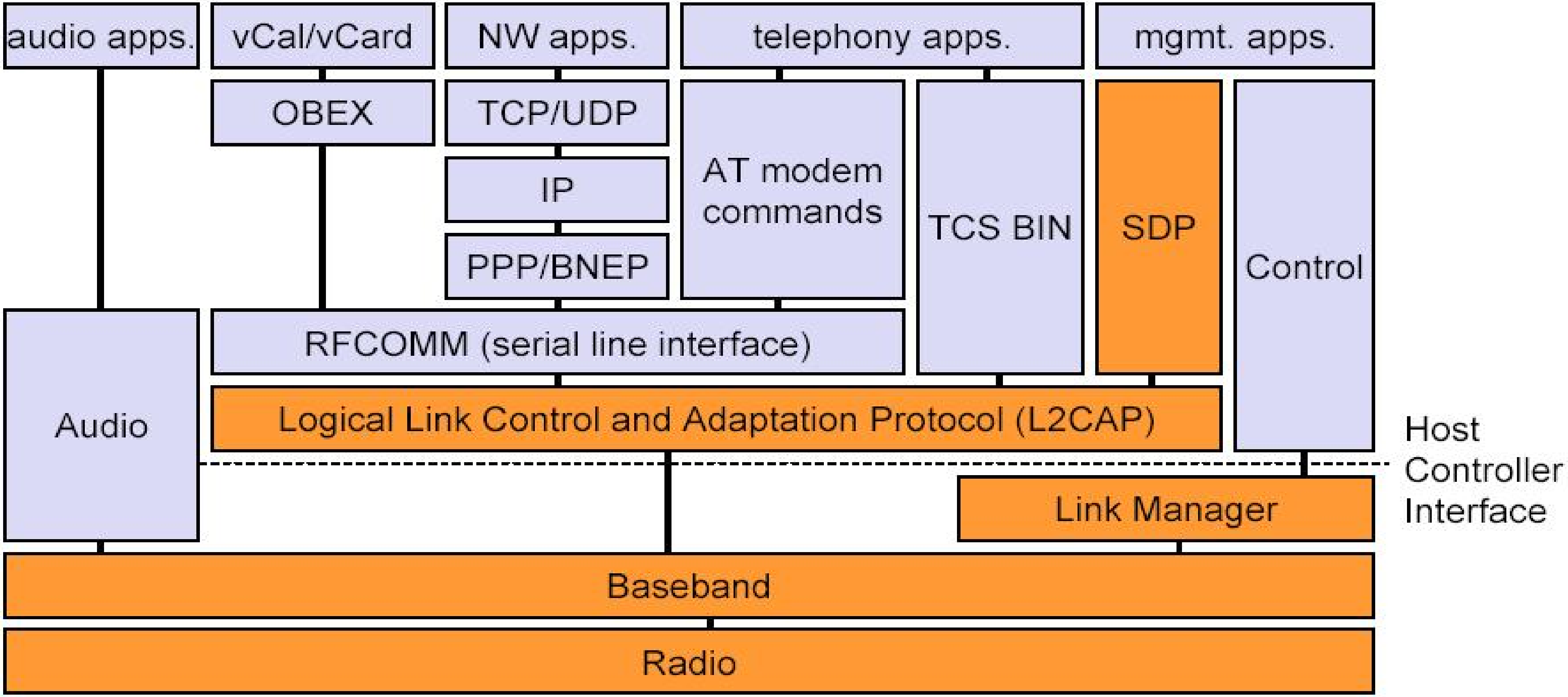
- Basic unit of Bluetooth networking
- Master and one to seven slave devices
- Master determines channel and phase

Scatternet



•Each connected radio can be a master “M” or slave “S” (ad-hoc)
•Radios can share piconets (scattered)
•“M” can connect 7 simultaneous active slaves in a pico-net
•If access is not available radios can go to standby “sb” mode waiting to join
•Up to 10 pico net can operate in one area
•A radio can be in a parked/hold, “P”, in a low power connection.

Technical Overview



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.

Protocol Architecture

- Bluetooth is a layered protocol architecture
  - Core protocols
  - Cable replacement and telephony control protocols
  - Adopted protocols
- Core protocols
  - Radio
  - Baseband
  - Link manager protocol (LMP)
  - Logical link control and adaptation protocol (L2CAP)
  - Service discovery protocol (SDP)

Protocol Descriptions

•LMP (link manager protocol) provides for link set-up: authentication and encryption, state of units in the piconet, power modes, packet size.

•L2CAP: Provides connection-oriented and connectionless data services to the upper layer protocols: protocol multiplexing, segmentation and reassembly, and group abstractions for data packets up to 64 kilobytes in length.

•SDP: service discovery protocol finds the characteristics of service and connects two or more Bluetooth devices to support the service.

•RFCOMM is a “cable replacement” protocol emulates RS-232 control and data signals over Bluetooth baseband.

•TCS: Telephony Control protocol defines the call control signaling for the establishment of speech and data calls. In addition, it defines mobility management procedures. It is based on the ITU-T Recommendation Q.931.

Supported Applications

With this architecture it supports:

• PPP: Point-to-Point Protocol;

•UDP/TCP: User Datagram Protocol /TCP;

•IP/TCP;

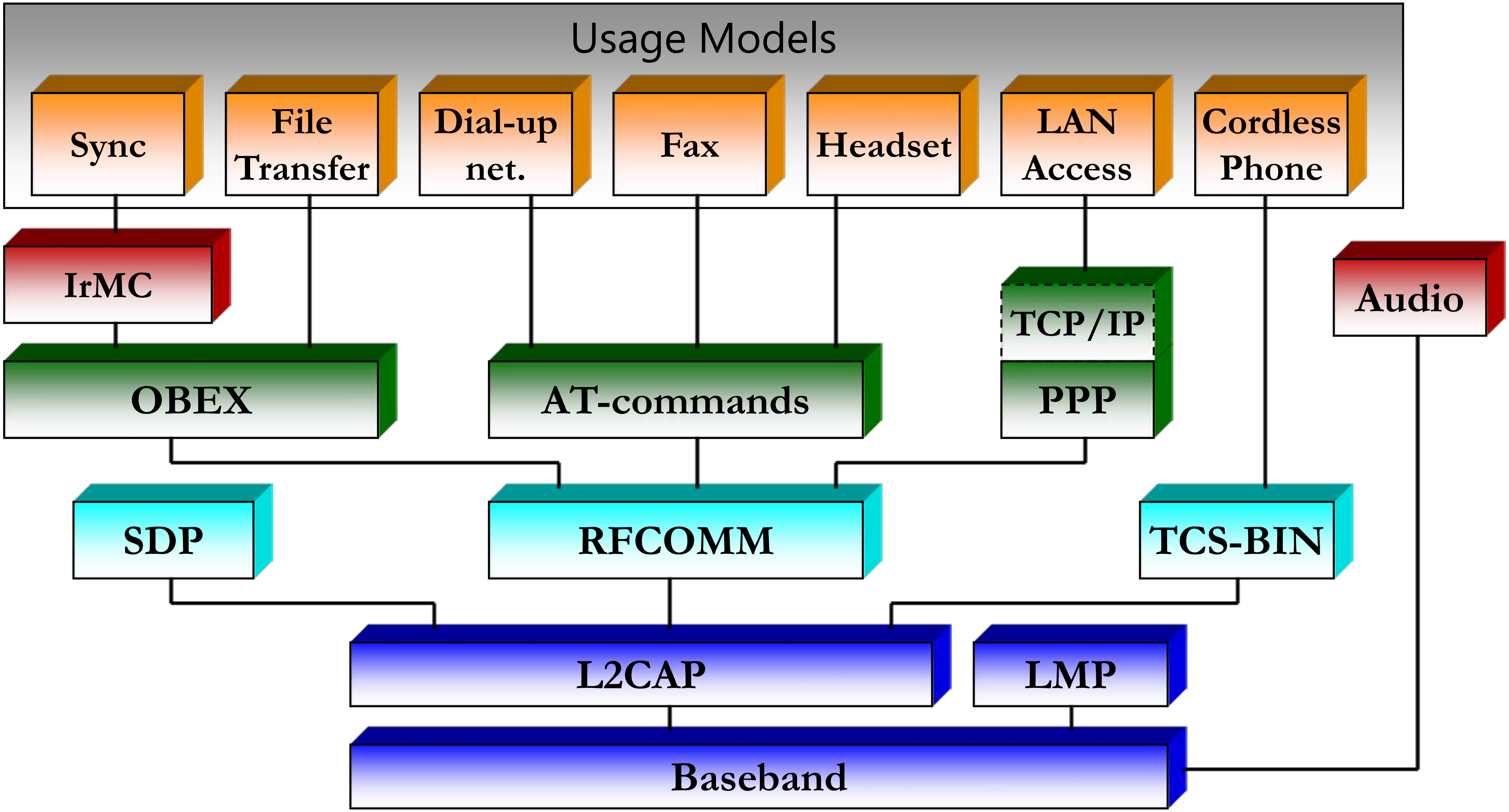
•WAP: Wireless Application Protocol;

•WAE: Wireless Application Environment;

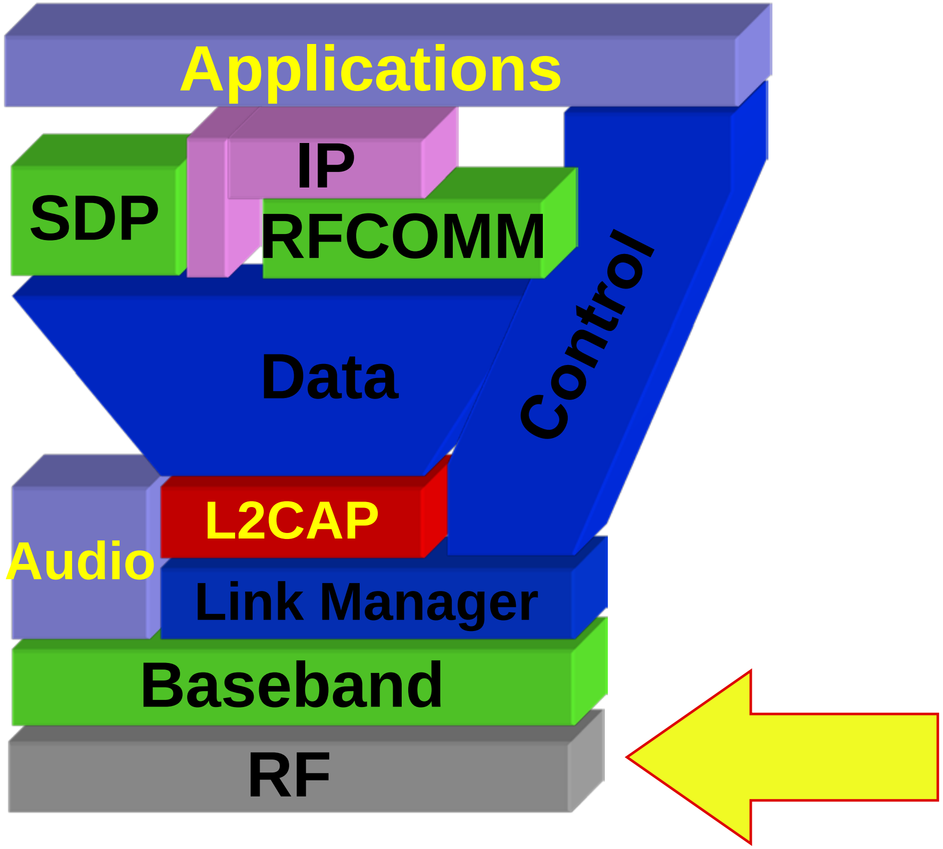
•OBEX (IR):Object Exchange Protocol;

•vCard/vCal: Virtual Card/ Calander.

Protocols and Usage Models



Bluetooth Radio Specification



0 dBm	Tx power
-20	Rx power @ 10 cm
-70	Rx power @ 10m
-91	Noise floor

C/I = 21 dB

Radio Specification - I

- Operates in 2.4GHz ISM bands (similar to 802.11)
- Transmission specification (Bluetooth 1.2)
  - Modem: 2 FSK modulation yields 432 kbit/s bidirectional / 721 kbit/s asymmetrical
  - Transmission rate: 1Mbps
  - Power: 0dBm (10m coverage) with an option for 20dBm (100m)
- *Fast* FH-CDMA/TDD (one packet per hop) for each piconet
  - 1600 hops per second (625µsec dwell time)
  - 79 hops (1MHz) available in ISM bands
  - Radios alternate between transmit and receive mode
  - At each slot “Master” decides and *polls* a “Slave”

Radio Specification -II

Bluetooth 2.0 + EDR

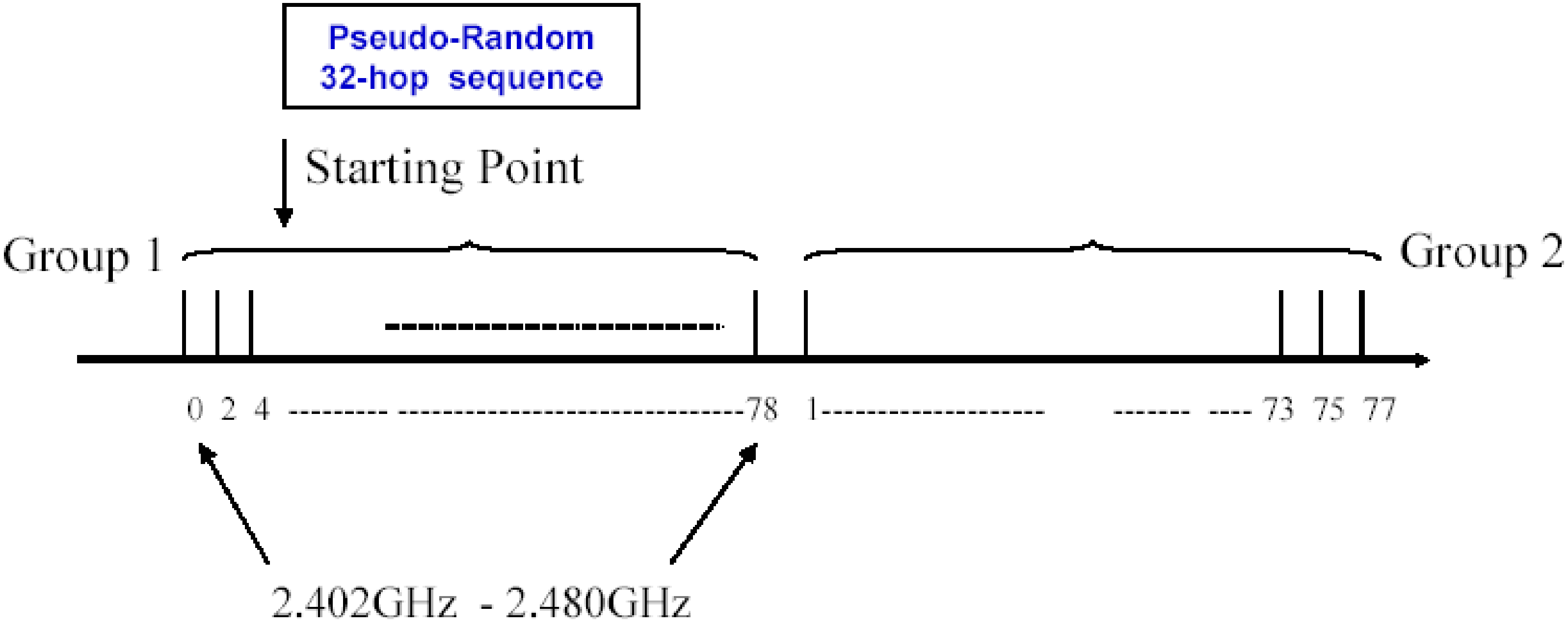
- **Enhanced Data Rates (EDR) bringing fast data transfer**
- **a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK**
- **rates of up to 2.1 Mbit/s.**
- **Reduced power consumption through a reduced duty cycle.**
-

Baseband Specification

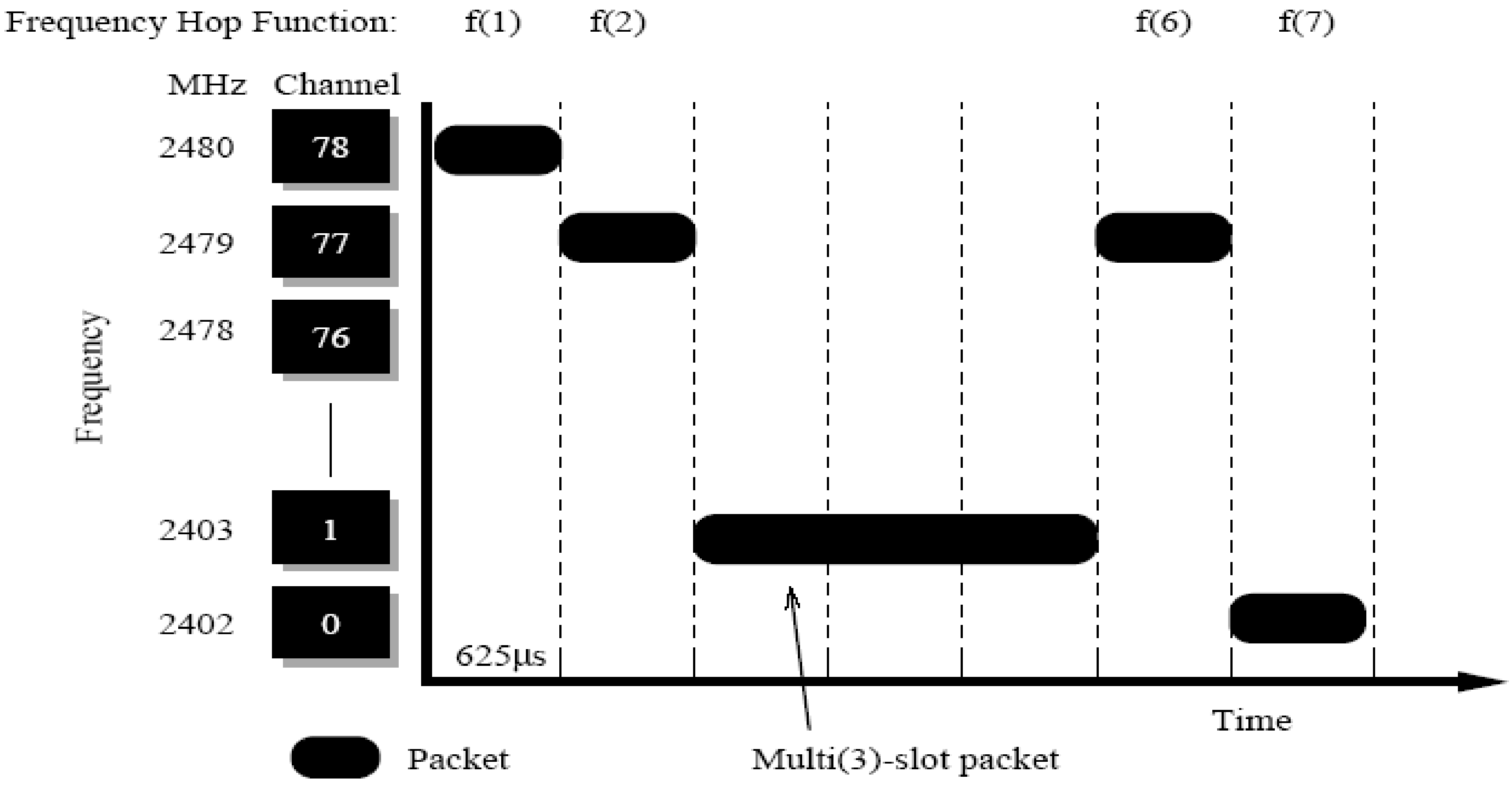
- Frequency hopping
- Physical links
- Packets
- Logical channels
- Channels control – State transition

Frequency Hopping in Bluetooth

- Provides resistance to interference and multipath effects
- Provides a form of multiple access among co-located devices in different piconets
- Two FH groups:

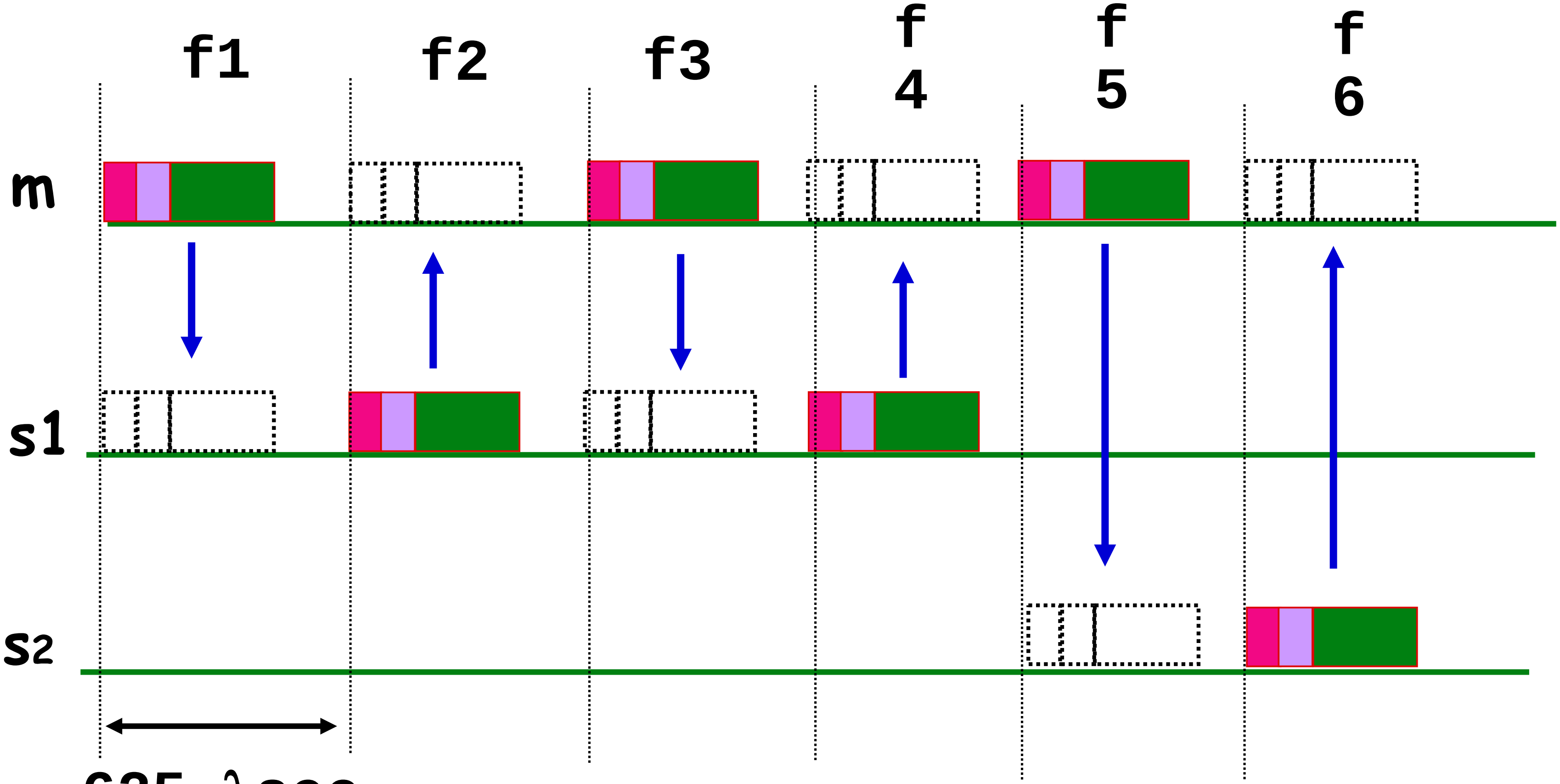


Frequency Hopping (cont.)



Piconet channel

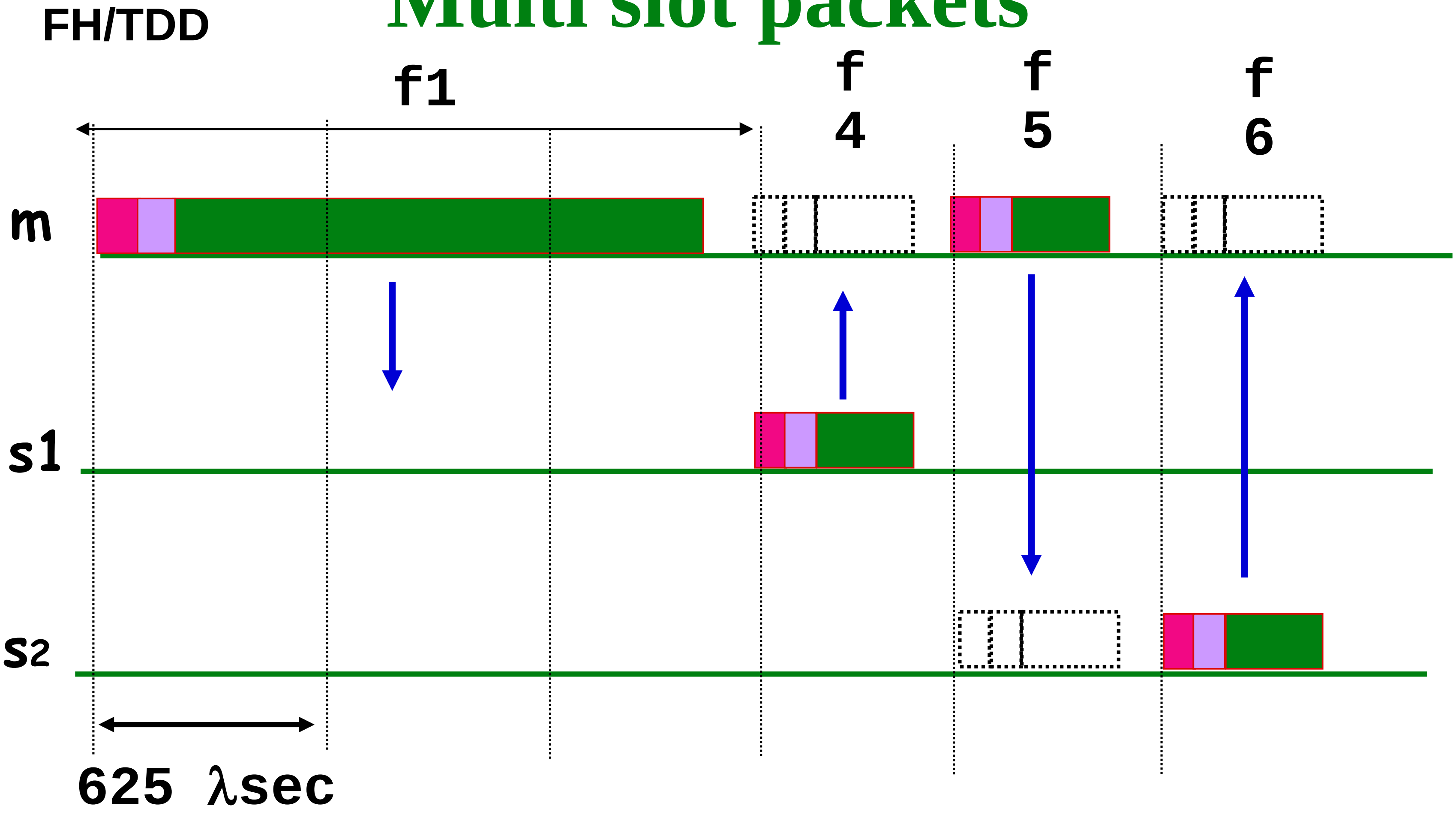
FH/TDD



625 λsec

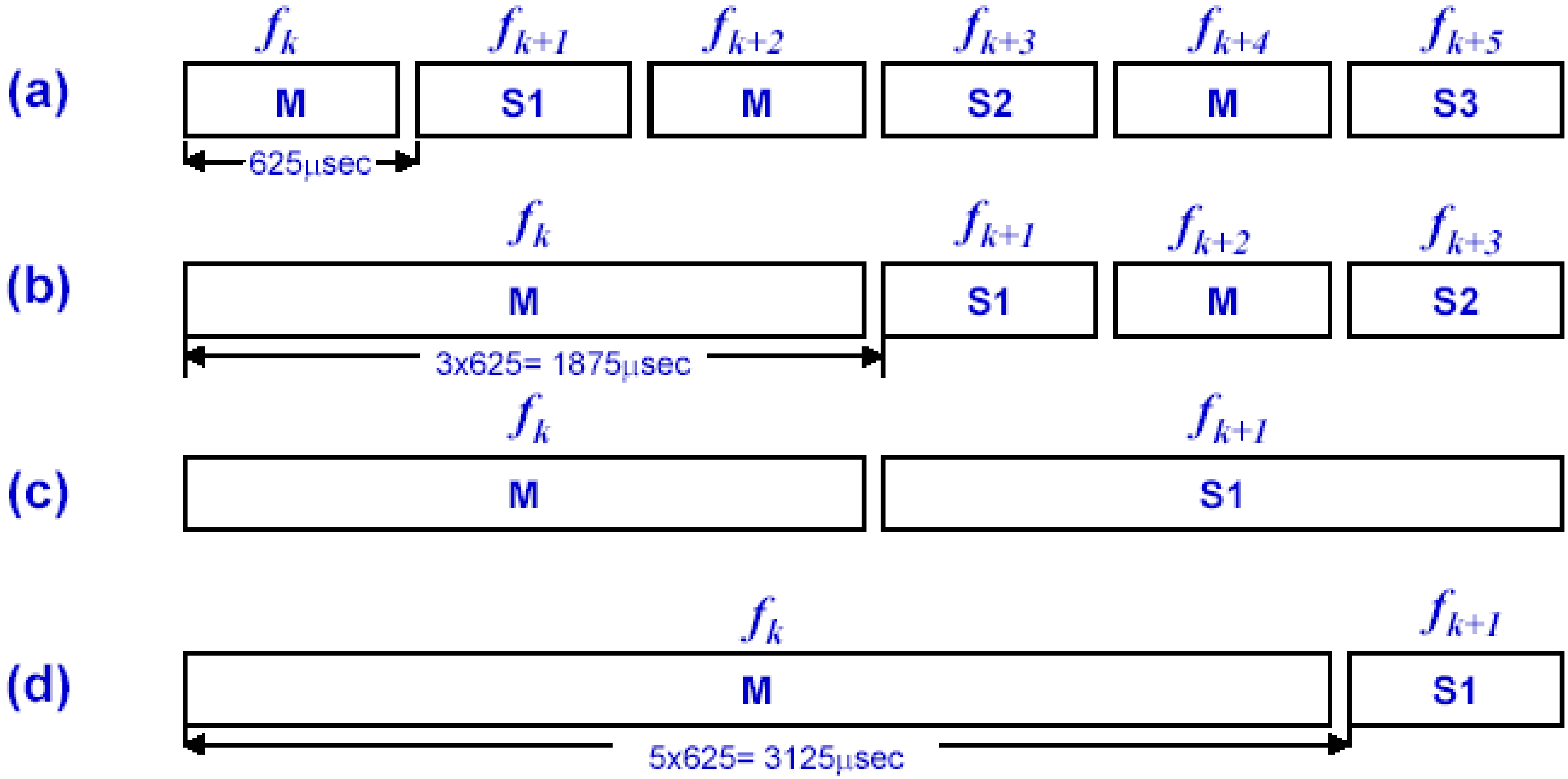
1600 hops/sec

Multi slot packets



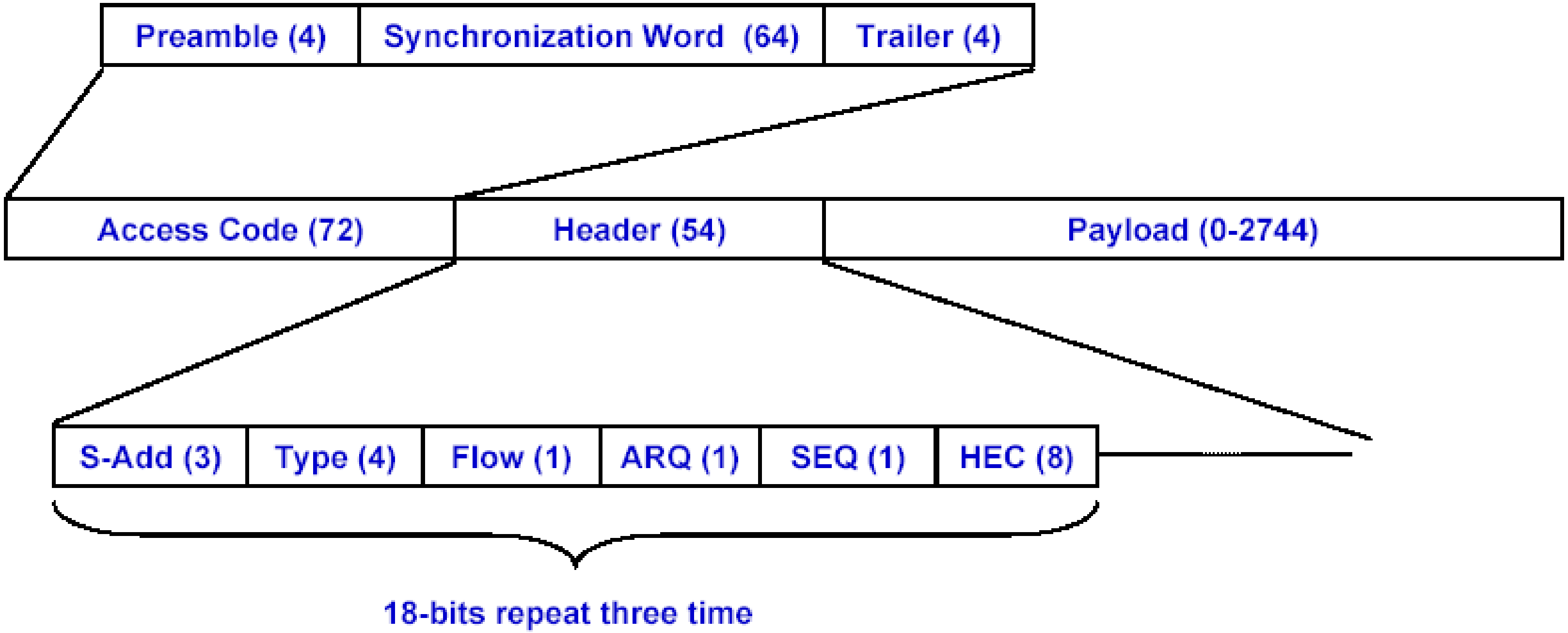
Data rate depends on type of packet

FH/TDMA/TDD Multislot Packet Format



Within each piconet, FH/TDMA/TDD is used for multi-user access!
(a) 1-slot packets (b) asymmetric 3-slot (c) symmetric 3-slots (1875µsec) (d) asymmetric 5-slot (3125µsec)

Bluetooth Packet Fields



- **Access code – used for timing synchronization, offset compensation, paging, and inquiry**
- **Header – used to identify packet type and carry protocol control information**
- **Payload – contains user voice or data and payload header, if present**

Field Format Description

Access code

- A PN sequence with piconet ID
- Slaves only accept packets with their Master's access code ID

Header (18-bits protected with 1/3 FEC codes)

- 3-bit Slave address
- 1-bit ACK/NACK for automatic repeat request (ARQ)
- 4-bit payload type (four control, 12 different services: sync/async-multiple slots)
- 8-bits CRC error correcting codes

Four control packets

- ID: only access code used for signaling
- NULL: access code and header, used to convey header
- POLL: similar to NULL with master request to response
- FHS: FH-Synchronization packet

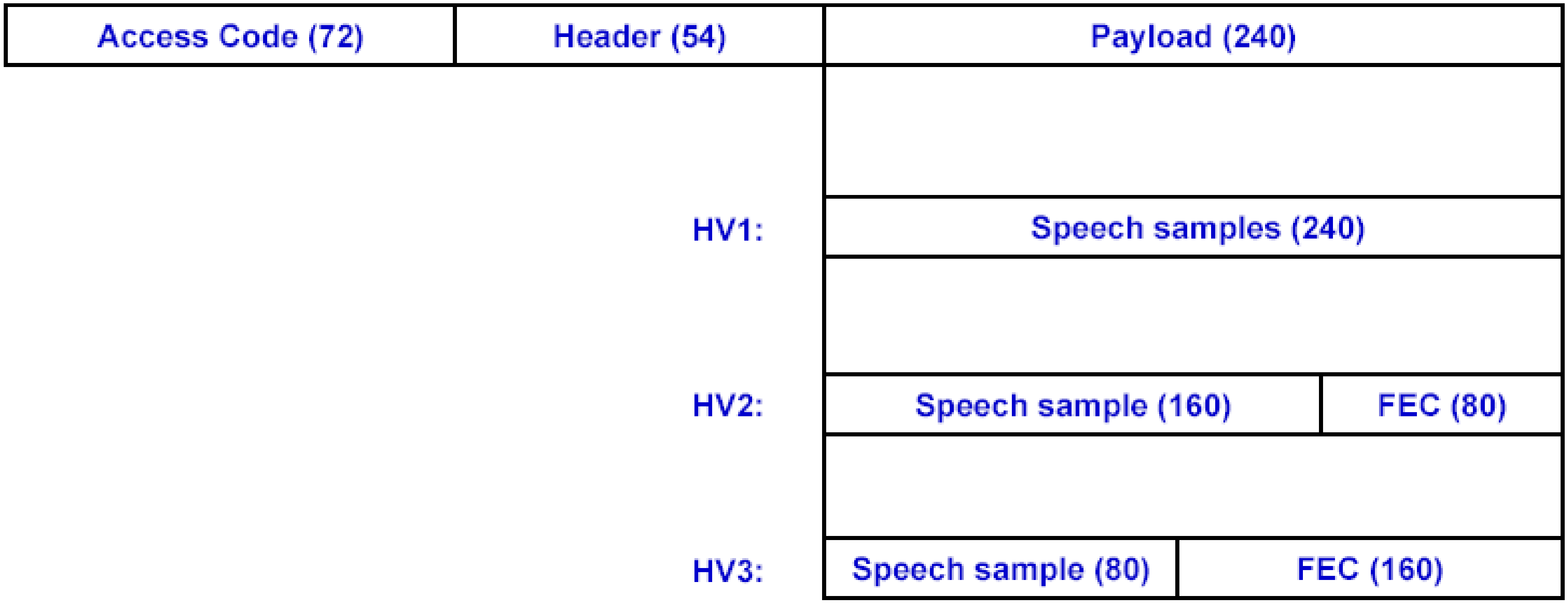
Error Correction Schemes

- 1/3 rate FEC (forward error correction)
  - Used on 18-bit packet header, voice field in HV1 packet
- 2/3 rate FEC
  - Used in DM packets, data fields of DV packet, FHS packet and HV2 packet
- ARQ
  - Used with DM and DH packets

Physical Links between Master and Slave

- Synchronous connection oriented (SCO)
  - Allocates fixed bandwidth between point-to-point connection of master and slave
  - Master maintains link using reserved slots
  - Master can support three simultaneous links
- Asynchronous connectionless (ACL)
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

SCO 1 Slot Packet Format



Access Code (72)

Header (54)

Payload (240)

HV1: Speech samples (240)

HV2: Speech sample (160) FEC (80)

HV3: Speech sample (80) FEC (160)

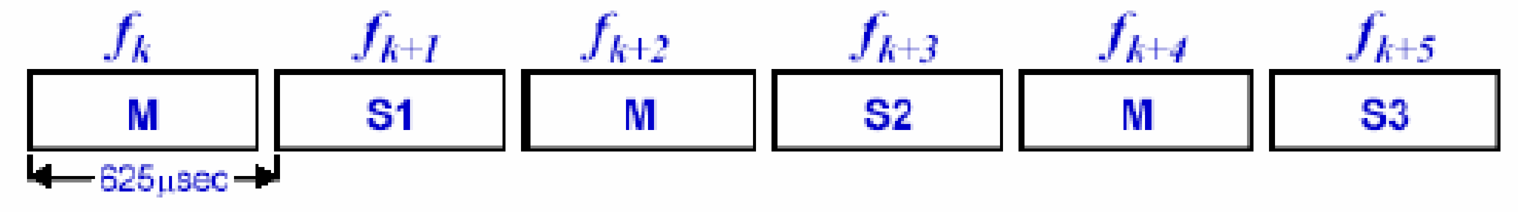
HV – High-quality Voice

SCO Data Rate example

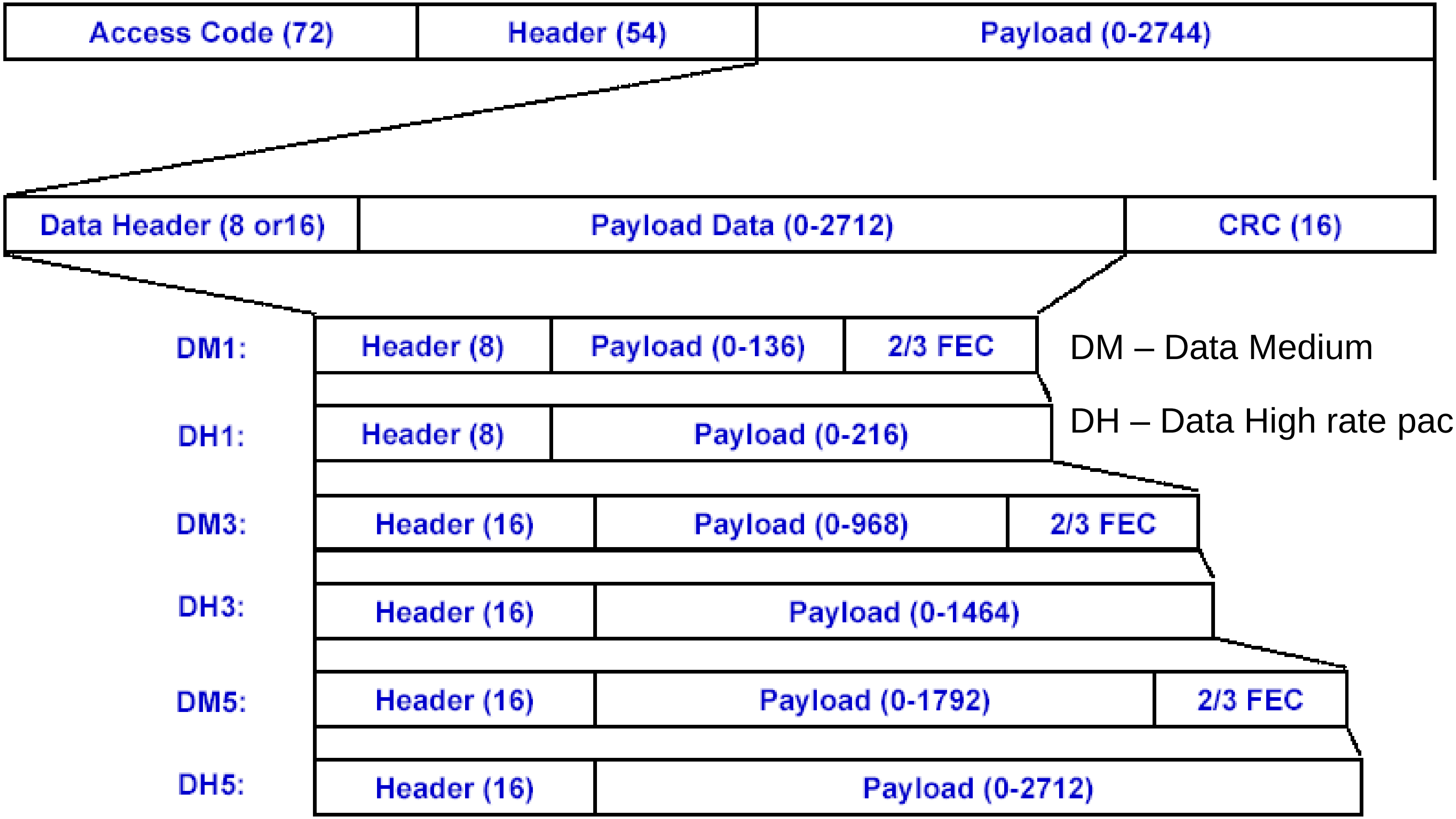
DATA RATE OF HIGH QUALITY VOICE PACKETS

THE HV1 PACKETS ARE 240 BITS LONG, AND SO THEY ARE SENT EVERY 6-SLOTS. THE PACKETS ARE 1-SLOT PACKETS SENT AT THE RATE OF 1600 SLOTS/SEC. THEREFORE, WE HAVE

$$(1600(slots\ /\mathrm{sec})/\ 6(slots))\times 240(bits) = 64Kbits\ /\mathrm{sec}\ .$$



ACL 1- 3- and 5- Slot Packet Format



Access Code (72) | Header (54) | Payload (0-2744)

Data Header (8 or16) | Payload Data (0-2712) | CRC (16)

DM1: Header (8) | Payload (0-136) | 2/3 FEC

DH1: Header (8) | Payload (0-216)

DM3: Header (16) | Payload (0-968) | 2/3 FEC

DH3: Header (16) | Payload (0-1464)

DM5: Header (16) | Payload (0-1792) | 2/3 FEC

DH5: Header (16) | Payload (0-2712)

DM – Data Medium

DH – Data High rate packets

ACL Data Rate examples

HIGH DATA RATE IN BLUETOOTH

A symmetric 1-slot DH1 link between an “M” and a “S” terminal carries 216 bits per slot at a rate of 800 slots per second (every other slot) in each direction. The associated data rate is $216(\mathit{bits} / \mathit{slot}) \times 800(\mathit{slots}/\mathrm{sec}) = 172.8(\mathit{Kb} / s)$.

MEDIUM DATA RATE IN BLUETOOTH

THE ASYMMETRIC DM5 LINK, SHOWN IN FIG 13.12D USES 5-SLOT PACKETS CARRYING 1792 BITS PER PACKET BY THE “M” AND 1-SLOT PACKET CARRYING 136 BITS PER PACKET BY THE “S” TERMINAL. THE NUMBER OF PACKETS PER SECOND IN EACH DIRECTION IS 1600/6 PACKETS PER SECOND. THEREFORE THE DATA RATE FROM “M” IS GIVEN BY:

$$1792(\mathit{bits} / \mathit{packet}) \times (1600/6\,\mathit{packets}/\mathrm{sec}) = 477.8(\mathit{Kb} / s)$$

THE DATA RATE OF THE “S” TERMINAL IN THIS ASYMMETRIC CONNECTION IS:

$$136(\mathit{bits} / \mathit{packet}) \times (1600/6\,\mathit{packets}/\mathrm{sec}) = 36.3(\mathit{Kb} / s)$$

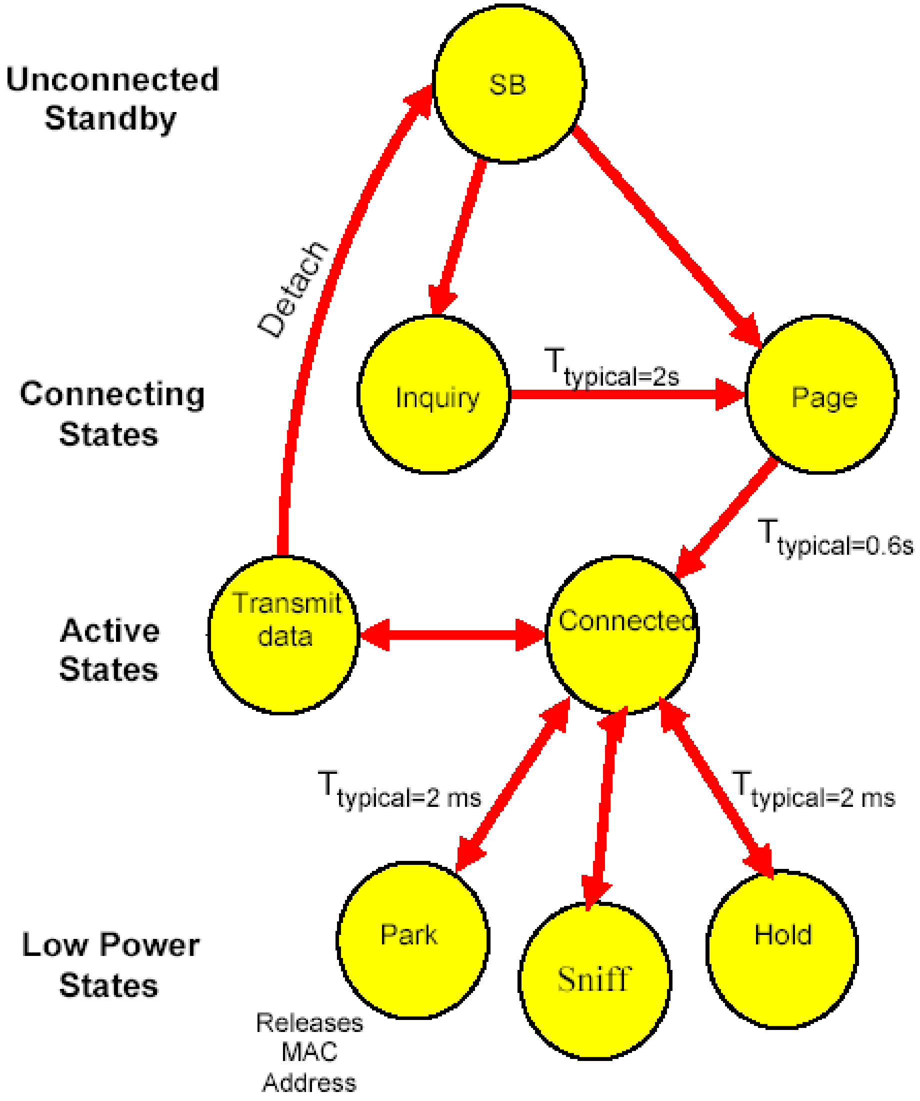
Logical Channels

Five logical channels in Bluetooth to carry different types of payload traffic:

- **Link control (LC)**
  - **Used to manage the flow of packets over the link interface**
- **Link manager (LM)**
  - **Transports link management information between participating stations**
- **User asynchronous (UA)**
  - **Carries asynchronous user data**
- **User isochronous (UI)**
  - **Carries isochronous user data**
- **Use synchronous (US)**
  - **Carries synchronous user data**

State Transition

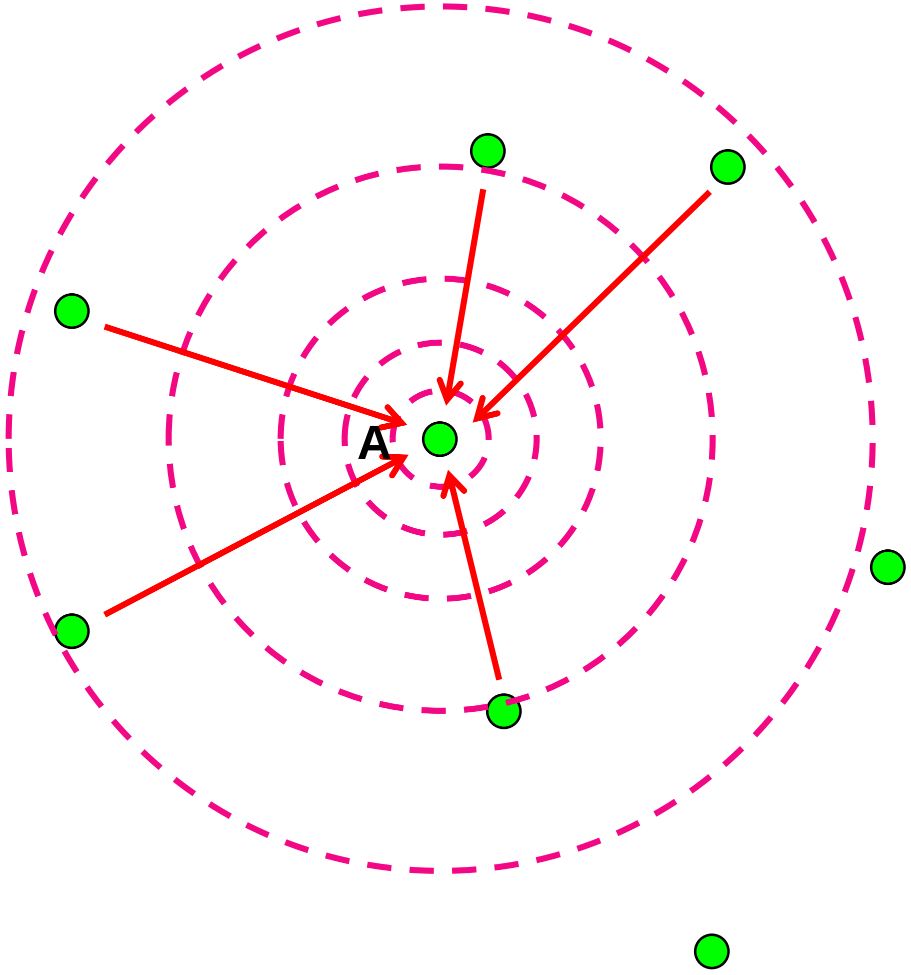
- **Standby**
  - Waiting to join a piconet
- **Inquire**
  - Ask about radios to connect to
- **Page**
  - Connect to a specific radio
- **Connected**
  - Actively on a piconet (master or slave)
- **Park/Sniff/Hold**
  - Low-power connected states



Addressing

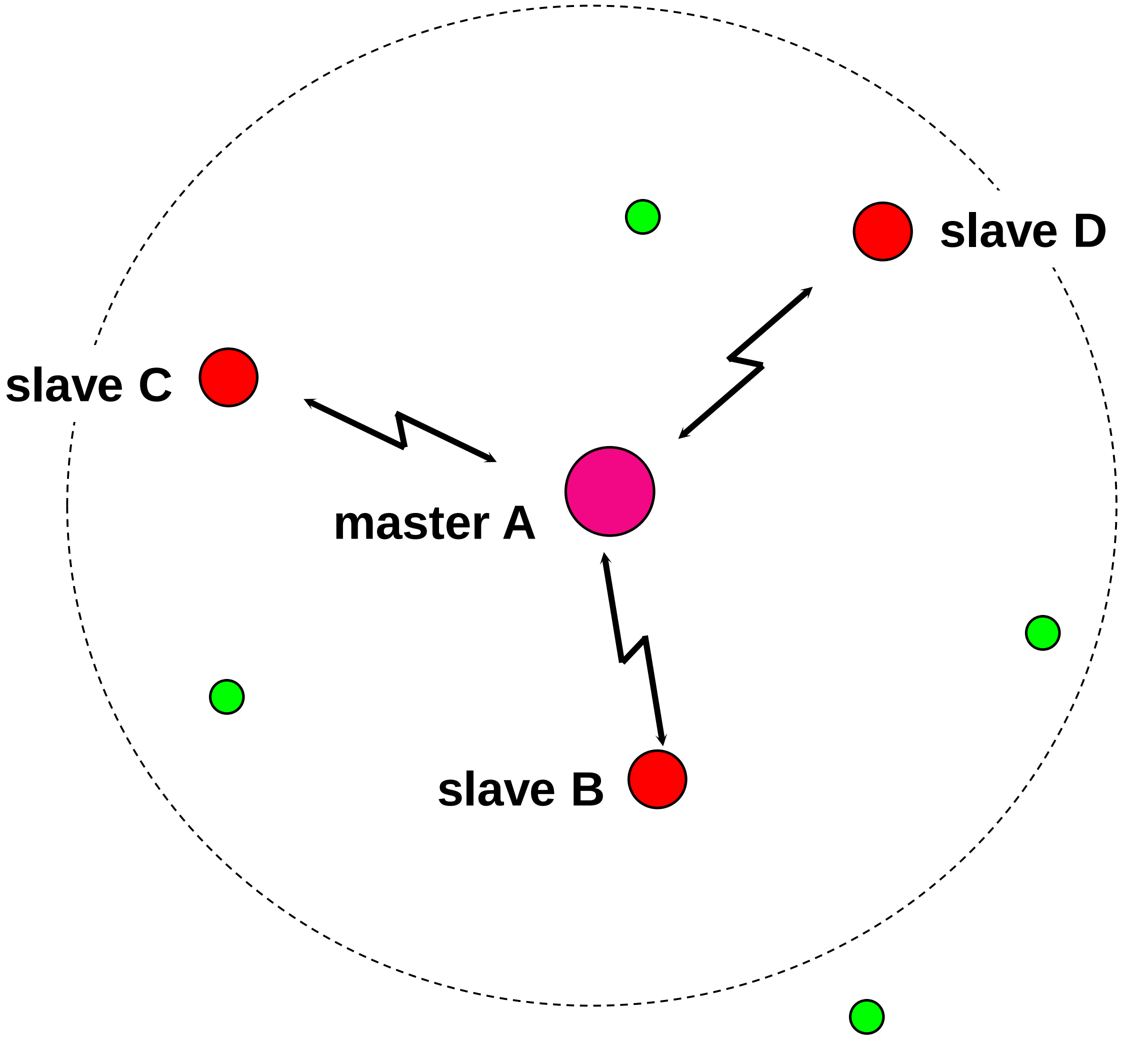
- Bluetooth device address (BD_ADDR)
  - 48 bit IEEE MAC address
- Active Member address (AM_ADDR)
  - 3 bits active slave address
  - all zero broadcast address
- Parked Member address (PM_ADDR)
  - 8 bit parked slave address

Inquiry



- **Purpose: Looking for Unknown Devices**
- **Responses include:**
  - **Device Address**
  - **Class of Device**

Paging



- Purpose: Establish Connection
- Done for each device independently
- Paging device becomes master

Connection management

- States of operation of a piconet during link establishment and maintenance
- Major states
  - Standby – default state
  - Connection – device connected

- Connection Process:
  - SB – all devices are in SB mode
  - Inquiry – one device starts with an inquiry and becomes ‘M’ terminal;

    – all ‘S’ terminals send ID and timing to ‘M’ terminal.
  - Page – ‘M’ terminal sends its ID and timing to ‘S’ terminals.
  - Connected – communication session takes place.

    - the terminal can sent back to SB, Hold, Park, Sniff states.

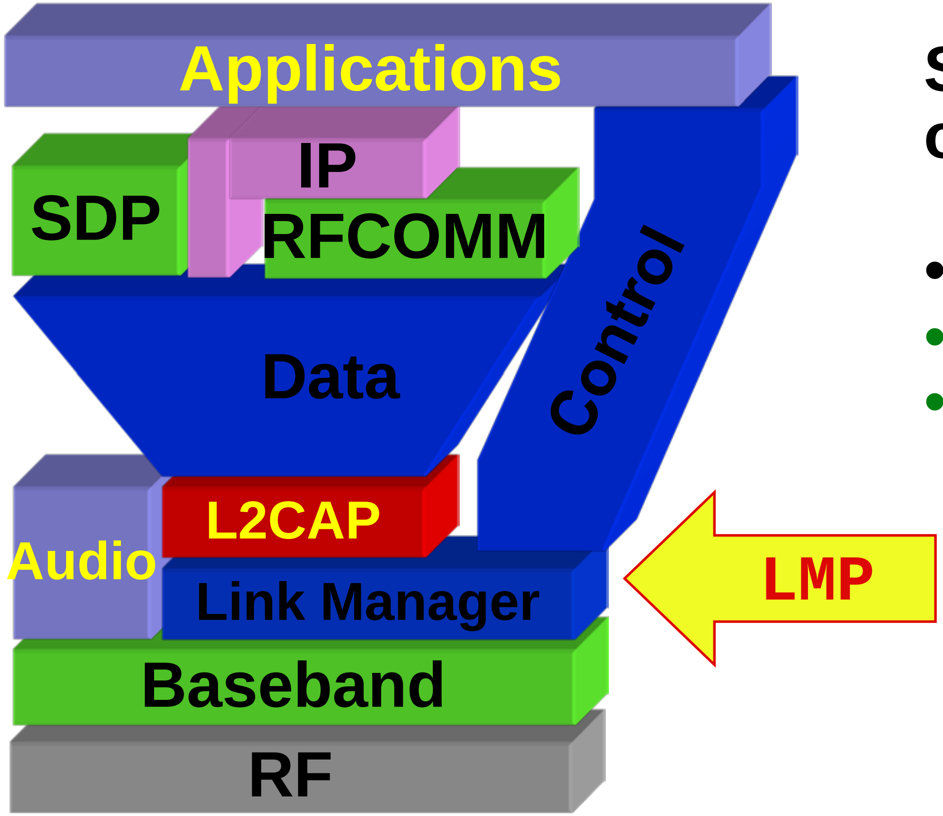
Slave Connection State Modes

- **Active – participates in piconet**
  - Listens, transmits and receives packets
- **Sniff – only listens on specified slots**
- **Hold – does not support ACL packets**
  - Reduced power status
  - May still participate in SCO exchanges
- **Park – does not participate on piconet**
  - Still retained as part of piconet

Bluetooth Audio

- **Voice encoding schemes:**
  - **Pulse code modulation (PCM)**
  - **Continuously variable slope delta (CVSD) modulation**
- **Choice of scheme made by link manager**
  - **Negotiates most appropriate scheme for application**

Link Manager Protocol



Setup and Management of Baseband connections

- Piconet Management
- Link Configuration
- Security

Link Manager Protocol

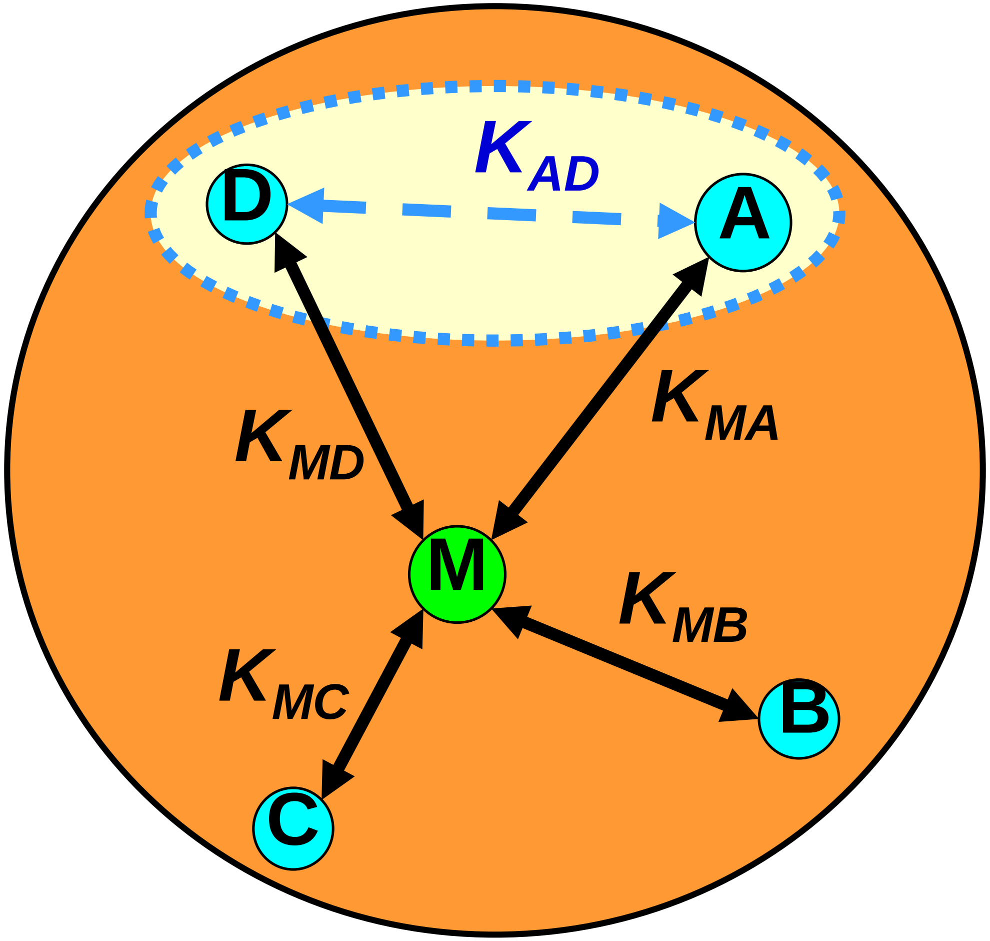
- Piconet Management
  - Attach and detach slaves
  - Master-slave switch
  - Establishing SCO and ACL links
  - Handling of low power modes (Sniff, Hold, Park)
- Link Configuration
  - packet type negotiation
  - power control
- Security functions
  - Authentication
  - Encryption

Bluetooth security features

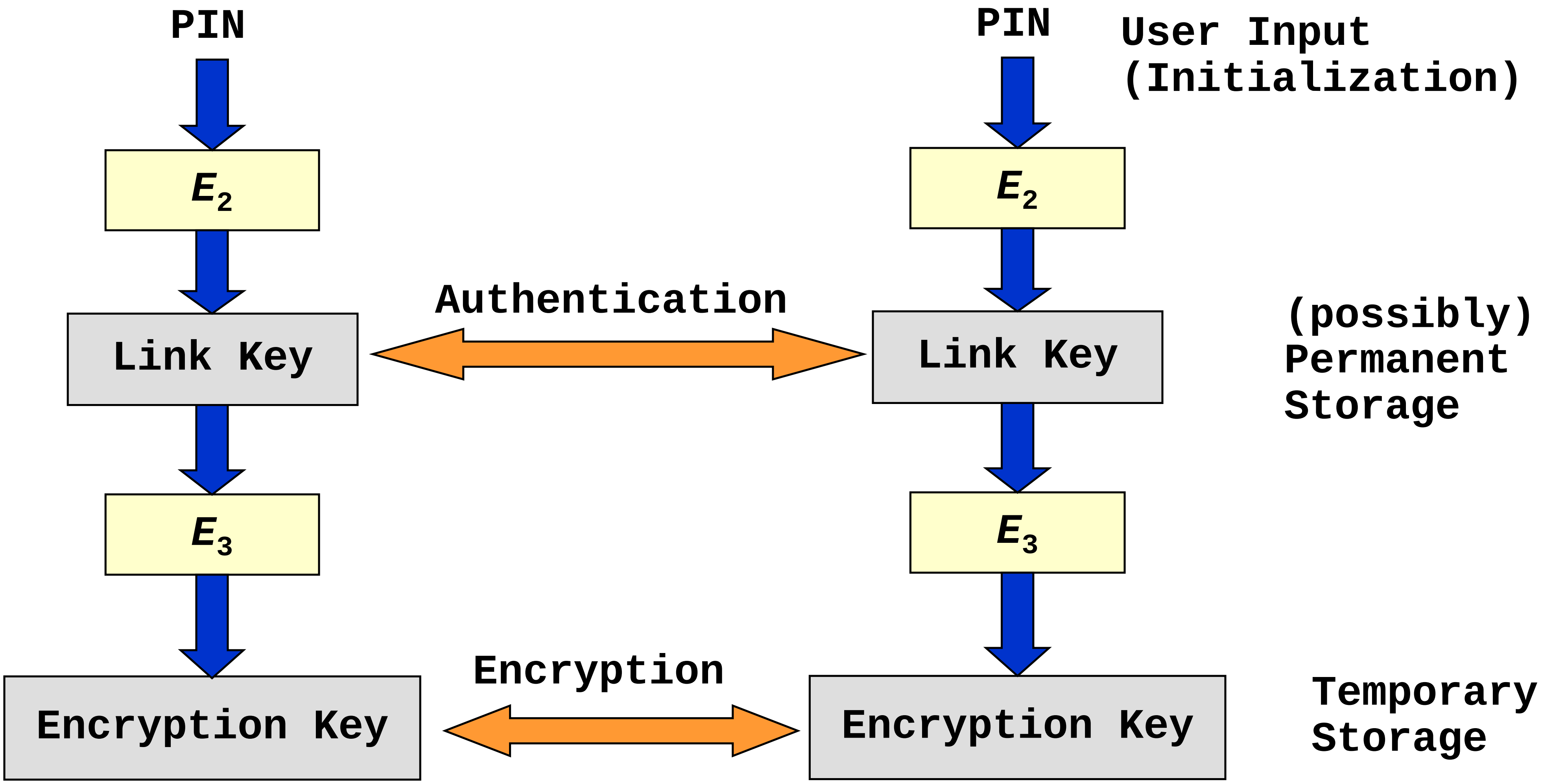
- Fast frequency hopping (79 channels)
- Low transmit power (range <= 10m)
- Authentication of remote device
  - based on link key (128 Bit)
  - May be performed in both directions
- Encryption of payload data
  - Stream cipher algorithm (≤ 128 Bit)
  - Affects all traffic on a link
- Initialization
  - PIN entry by user

Link keys in a piconet

- Link keys are generated via a PIN entry
- A different link key for each pair of devices is allowed
- Authentication:
  - Challenge-Response Scheme
- Permanent storage of link keys



Key generation and usage



Application level security

- Builds on-top of link-level security
  - creates trusted device groups
- Security levels for services
  - authorization required
  - authentication required
  - encryption required
- Different or higher security requirements could be added:
  - Personal authentication
  - Higher security level
  - Public key

Class Quiz

- What is the network topology in Bluetooth?
- What is media access in Bluetooth?
- What is the state transition in Bluetooth?