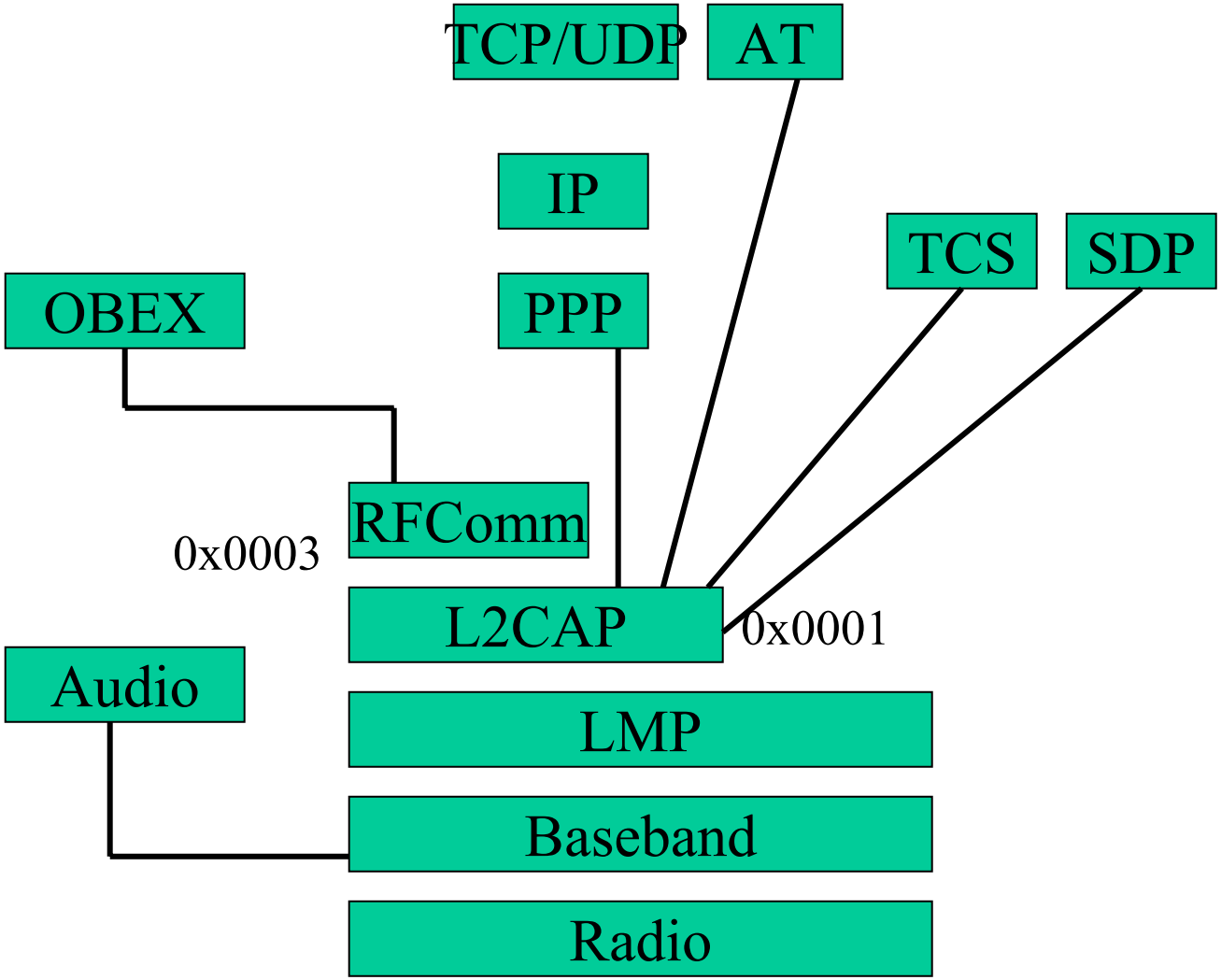
Bluetooth Technology

Sources:

BLUETOOTH, J Bray and C. F. Sturman
Bluetooth Baseband Specification

Bluetooth

- Low-power, short range, wireless radio system (BT SIG: Ericsson, Nokia, IBM, …)
- 10 m, 1-Mbps links to 7 BT devices, 2.4 GHz,
- Both isochronous and asynchronous traffic



Bluetooth Protocol Stack

BT Protocol Stack

- Radio+Baseband: Frequency hopping radio platform.
- LMP: Data link setup, authentication
- L2CAP: Multiplexed comm. (conn./less), proprietary
- RFComm: Emulates RS-232 serial interface
- OBEX: Object exchange protocol
- SDP: Service discovery protocol

BT Service Discovery Protocol (SDP)

- API for enumerating and browsing
- Stop rules to limit duration of searches
- Applications use API to search devices
  - By service classes (printer, storage, …)
  - By matching attributes (model #, protocol, …)
- Service attributes are managed as a record by the devices SDP server
- No mechanism for using discovered service

Radio (ISM band)

- 2.4000—2.4835 GHz frequency range
- 2 MHz Lower Guard Band
- 3.5 MHz Upper Guard Band
- Available channels 79

2.4465—2.4835 GHz freq range

7.5 MHz lower guard, 7.5 MHz upper guard,

23 channels

Device Address

- Bluetooth device address: 48 bits
  - BD_ADDR[23-:0] ← LAP[23:0] : freq hop
  - BD_ADDR[31-24] ← UAP[7:0] : freq hop
  - BD_ADDR[47-32] ← NAP[15:0] : encryption

Masters, Slaves, and Piconets

- BT is a TDM system
- Basic unit of op. is a 625 microsec slot
- In pre-connection stage (inquiry/page/scan), Tx and Rx can occur in half slots.
- In connection state, Tx and Rx can occur in multiple slots: 1, 3, 5.

BT Piconet

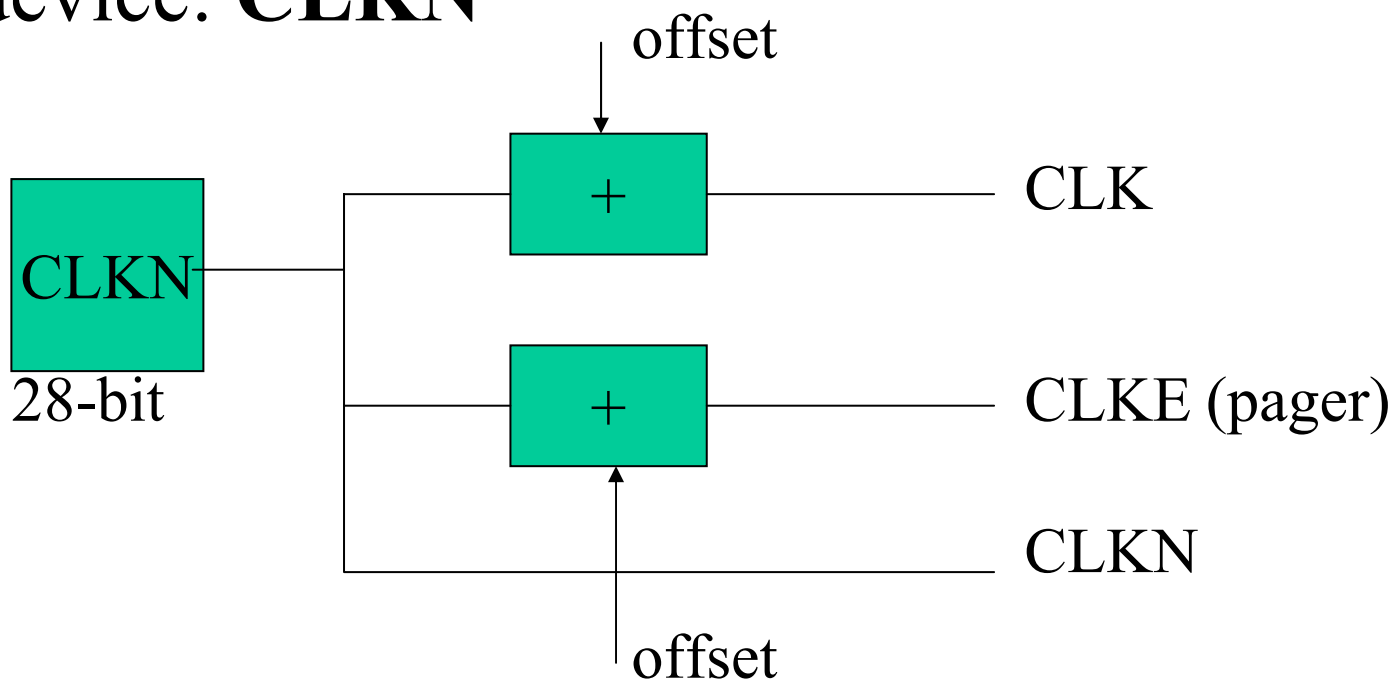
- Piconet: An ad hoc net of up to 8 BT devices
- Master:
  - The device which initiates an exchange of data
  - Coordinates devices in a piconet
- Devices can be a part of several piconets at the same time: scatternet

Device state

- Device state:
  - Standby (waiting to connect to another device)
  - Inquire (searching for nearby devices), Inq. Scan
  - Page (connecting to another device), Page Scan
  - Connect
  - Hold and park (Connected to a piconet, power saving)
    - Hold ➔ no ACL traffic, free up bandwidth for other ops. (scanning, paging, inquiry, low-power sleep ….)

Bluetooth Clock

- Every device has a free-running "native" clock that controls the timing and op of that device: **CLKN**



Physical Links: ACL, SCO

- ACL
  - It exists as soon as a connection is established.
  - 1 ACL link between a Master ←→ Slave
  - View it as a packet-switched connection.
  - Under the control of the Master: a Slave can only respond if it has been addressed by the Master in the preceding M-to-S slot.
  - Broadcast packets are ACL packets.

Physical Link: ACL, SCO

- SCO
  - Provides a symmetric link between Master/Slave
  - Reserved channel bandwidth (reserved slots)
  - Up to 3 SCO links between Master ←→ 1 or more slaves.
  - SCO packets are never retransmitted
  - A SCO link is set up by a Link Manager (LM) command from Master to Slave
  - Master transmits SCO packets to Slave at regular intervals, defined by T_{SCO}.

Packet Structure

- Packet
  - Access code: packet presence, from address
  - Header: control info (slave id)
  - Payload

Access Code

- CAC: derived from LAP of Master. Used by all in the piconet.
- DAC: derived from a device's LAP. Used by a paging device.
- GIAC: Used by all during inquiry. 0x9E8B33 ← fixed
- Dedicated IAC: 0x9E8B00—0x9E8B3F

Packet Header (18 bits)

- AM_ADDR (3 bits): 7 slaves, 1 bcast, at paging.
- Packet Type (4 bits) NULL, POLL, FHS, DM1..
- Flow (1 bit) : Set by a device when it is unable to receive more data due to lack of local buffer
- ARQN (1 bit) : Set by a device to indicate that the previous reception was OK.
  (Lost ARQN ➔ NACK)
- SEQN (1 bit): toggles for each new packet
- HEC (8 bits):

ACL Payload

- Payload Header
  - L_CH (2 bits): Start/continuation of L2CAP message or an LMP message
  - Flow (1 bit): L2CAP flow control
  - Length (9 bits): payload data length **in bytes**
  - Unused (3 bits)
- Payload: Up to 341 bytes
- CRC: 16 bits

SCO Packet Structure

- Access Code: similar to ACL packet's
- Header: similar to ACL packet's
- Payload: fixed 30 bytes (source data of 10, 20, or 30 bytes with 1/3, 2/3, or none encoding)

Packet Type Summary

Code	Slots	SCO	ACL	PLHB	UPLB	FEC	CRC
-	0.5	ID	ID	0	0		
0000	1	NULL	NULL	0	0		
0001	1	POLL	POLL	0	0	2/3	
0010	1	FHS	FHS	0	18		
0011	1	DM1	DM1	1	0-17	2/3	Yes
0100	1		DH1	1	0-27		Yes
0101	1	HV1		No	10	1/3	
0110	1	HV2		No	20	2/3	
0111	1	HV3		No	30		

Packet Type Summary (Contd.)

Code	Slots	SCO	ACL	PLHB	UPLB	FEC	CRC
1000	1	DV		1	10 (0-9)	2/3	Yes
1001	1		AUX1	1	0-29		
1010	3		DM3	2	0-121	2/3	Yes
1011	3		DH3	2	0-183		Yes
1100	3	xxxxxx	xxxxx				
1101	3	xxxxxx	xxxxx				
1110	5		DM5	2	0-224	2/3	
1111	5		DH5	2	0-339		Yes

Data Rates (ACL packets)

Type	UPLB	Symmetric Max rate (**kb/s**)	Asym. Max Rate **Forward**	
DM1	0-17	108.8	108.8	
DH1	0-27	172.8	172.8	
DM3	0-121	258.1	387.2	
DH3	0-183	390.4	585.6	
DM5	0-224	286.7	477.8	
DH5	0-339	433.9	723.2	
AUX1	0-29	185.6	185.6	

Calculation of data rates

Consider DM1 packet type:

User Payload (bytes) = 0-17

Symmetric Max. rate = 108.8 kb/sec

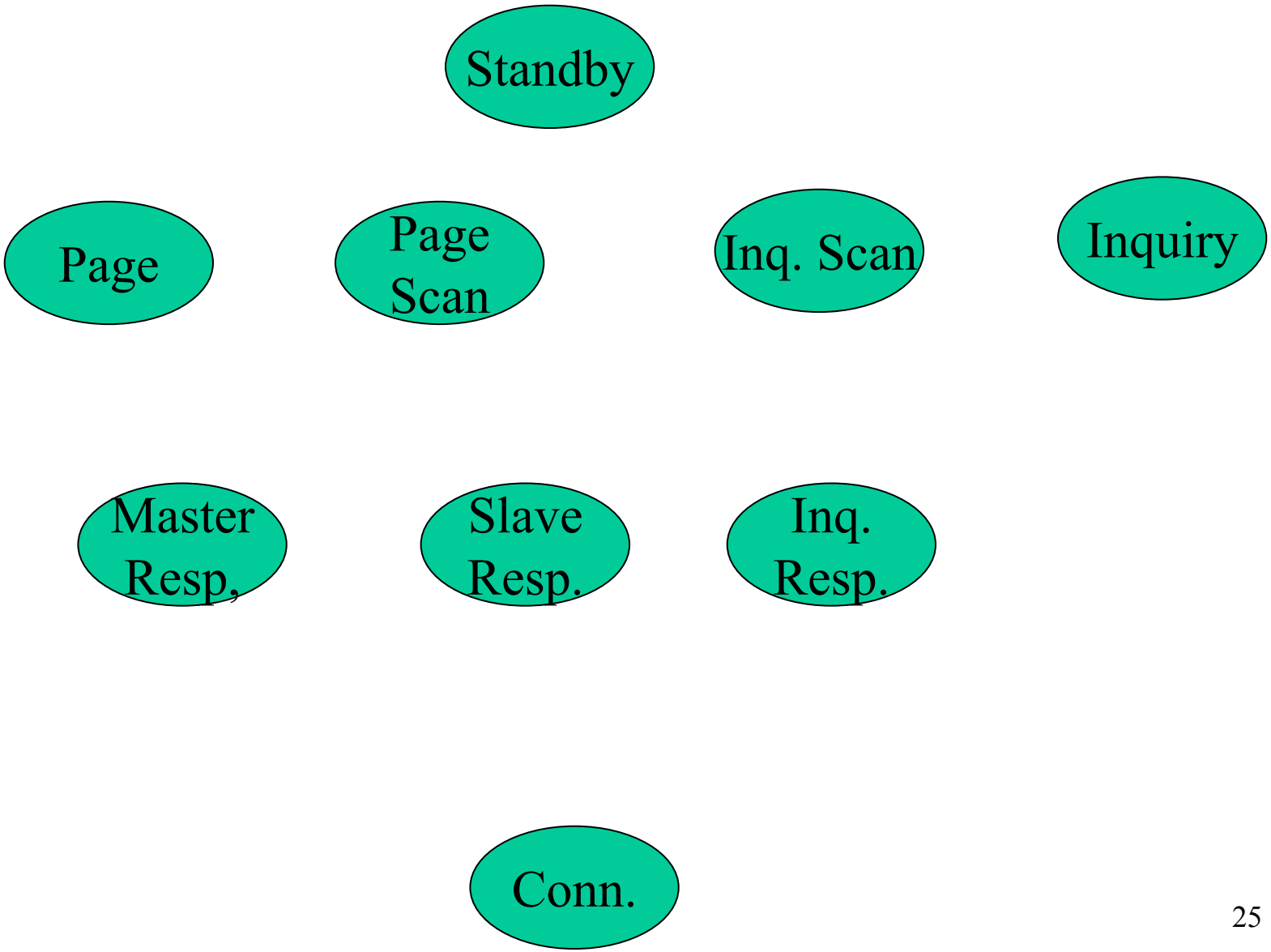
Data Rates (SCO packets)

Type	UPLB	Symmetric Max Rate (kb/s)
HV1	10 (FEC = 1/3)	64.0
HV2	20 (FEC = 2/3)	64.0
HV3	30 (no FEC)	64.0
DV	10 + (0-9) D	64.0 + 57.6 D

Logical Channels (Use of different packets)

- Link Control data: Packet header, ARQ, SEQ
- Link Manager data: Carried via DM1. L_CH = 11
- User Async data: Carried via ACL payload and contains L2CAP user data.
- User Sync data: Carried via SCO channel payload

Link Controller Operation



To be discussed in class

- Frequency hopping mechanism
- Inquiry protocol
- Paging protocol
- Some performance data