The University of Rhode Island

ELE 437
Introduction to Bluetooth

Overview

- ➢Overall introduction of bluetooth
- ➢Bluetooth Protocol Stack
  - ➢Physical Layer
  - ➢Baseband
  - ➢Link Manager Protocol (LMP)
  - ➢L2CAP
  - ➢RFCOMM

What is Bluetooth

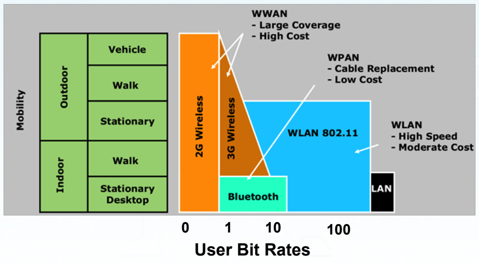
- ➢ It is a specification that attempts to provide a standard method of wireless communication between various personal devices
- ➢ Devices with ranging complexity can utilize Bluetooth technology: from cellular telephones to laptop computers
- ➢ Has a complete software framework and its own protocol stack.
- ➢ Specifications are driven by a Consortium that was founded in 1998 by Ericsson Microelectronics,Nokia, IBM, Toshiba and Intel. http://www.bluetooth.org

Goals of Bluetooth

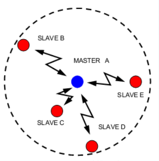
Ericsson Technology Licensing | Bluetooth Intellectual Property
making Bluetooth Dreams come true

- ➢Cable replacement
- ➢Low Cost (a $5 solution)
- ➢Low Power
- ➢Small Size
- ➢Dynamic networking for devices that are constantly mobile (not in motion)

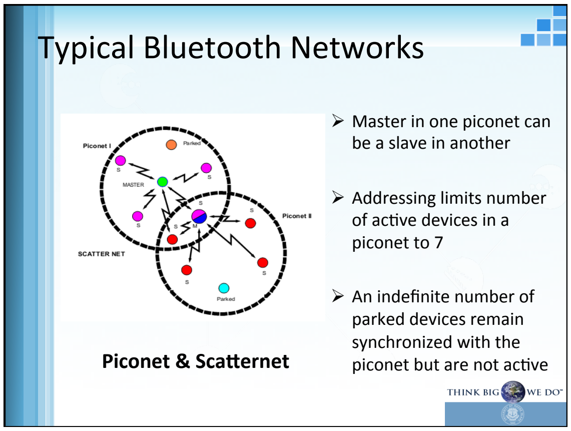
Different Wireless Protocols



Master/Slave Piconet



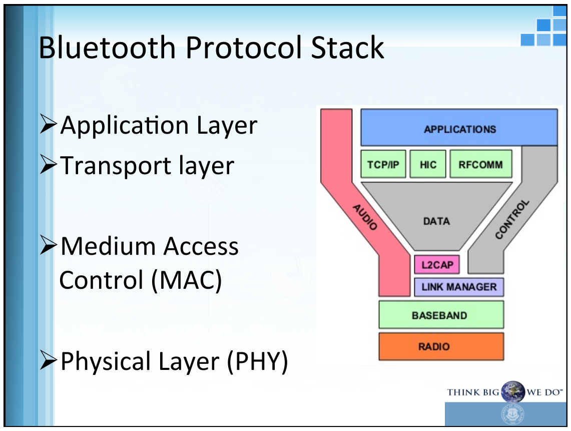
- ➢ Hopping sequence is unique for a piconet and is determined by the Master's BT address.
- ➢ The piconet is synchronized by the system clock of the Master.
- ➢ A slave can become a master in another Piconet. This connects two Piconets into a Scatter Net



Typical Bluetooth Networks

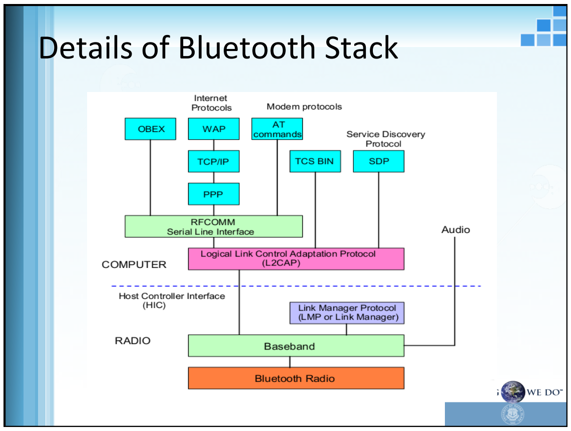
Piconet & Scatternet

- Master in one piconet can be a slave in another
- Addressing limits number of active devices in a piconet to 7
- An indefinite number of parked devices remain synchronized with the piconet but are not active



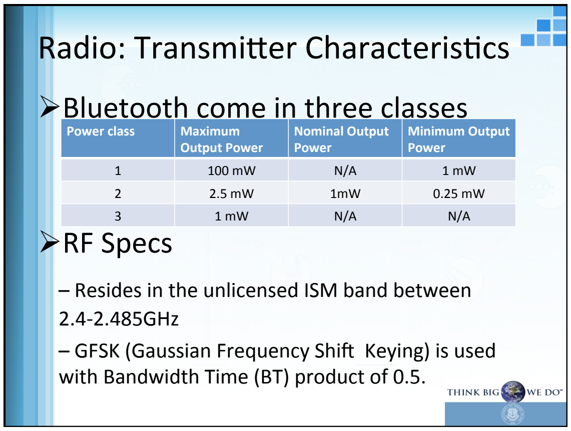
Bluetooth Protocol Stack

- Application Layer
- Transport layer
- Medium Access Control (MAC)
- Physical Layer (PHY)



Details of Bluetooth Stack

Internet Protocols
Modem protocols
OBEX
WAP
AT commands
Service Discovery Protocol
TCP/IP
TCS BIN
SDP
PPP
RFCOMM Serial Line Interface
Audio
Logical Link Control Adaptation Protocol (L2CAP)
COMPUTER
Host Controller Interface (HIC)
Link Manager Protocol (LMP or Link Manager)
RADIO
Baseband
Bluetooth Radio

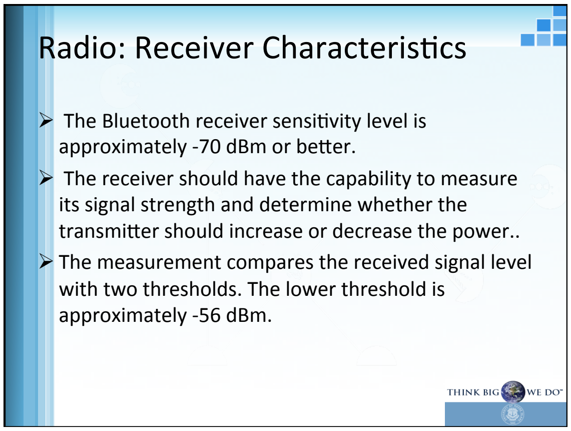


Radio: Transmitter Characteristics

- Bluetooth come in three classes

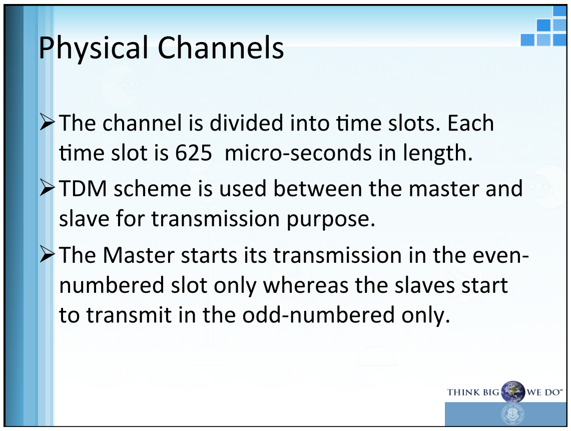
Power class	Maximum Output Power	Nominal Output Power	Minimum Output Power
1	100 mW	N/A	1 mW
2	2.5 mW	1mW	0.25 mW
3	1 mW	N/A	N/A

- RF Specs
  - – Resides in the unlicensed ISM band between 2.4-2.485GHz
  - – GFSK (Gaussian Frequency Shift Keying) is used with Bandwidth Time (BT) product of 0.5.



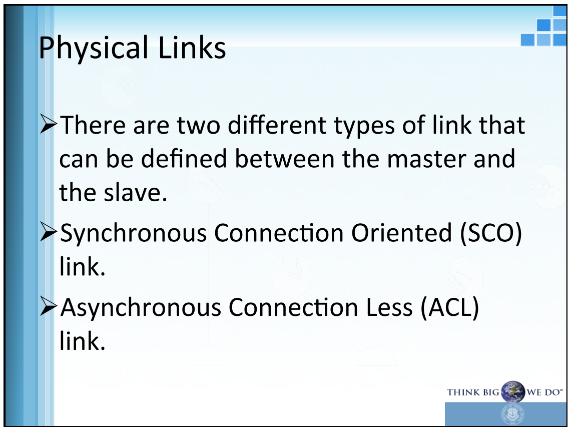
Radio: Receiver Characteristics

- The Bluetooth receiver sensitivity level is approximately -70 dBm or better.
- The receiver should have the capability to measure its signal strength and determine whether the transmitter should increase or decrease the power..
- The measurement compares the received signal level with two thresholds. The lower threshold is approximately -56 dBm.



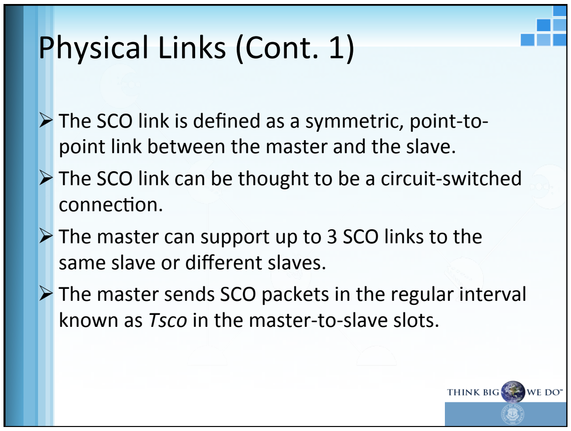
Physical Channels

- The channel is divided into time slots. Each time slot is 625 micro-seconds in length.
- TDM scheme is used between the master and slave for transmission purpose.
- The Master starts its transmission in the even-numbered slot only whereas the slaves start to transmit in the odd-numbered only.



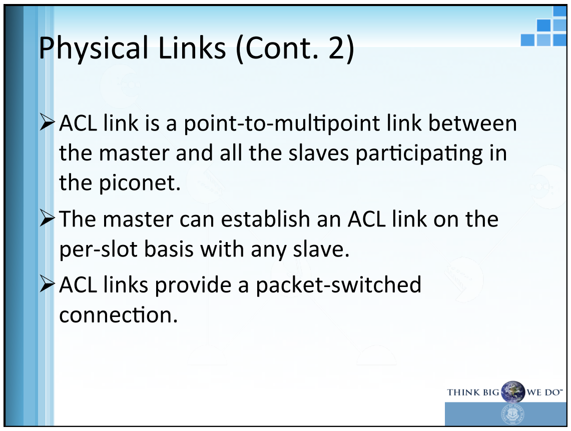
Physical Links

- There are two different types of link that can be defined between the master and the slave.
- Synchronous Connection Oriented (SCO) link.
- Asynchronous Connection Less (ACL) link.



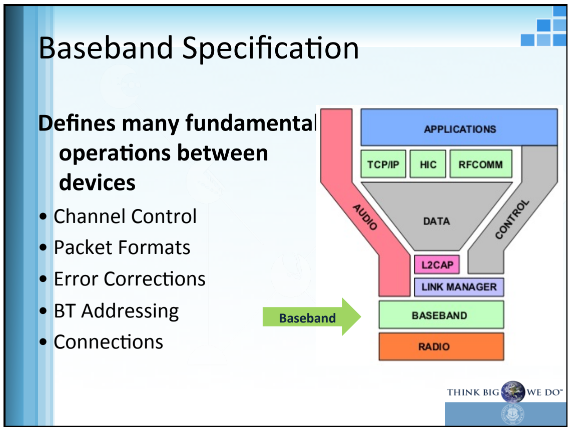
Physical Links (Cont. 1)

- The SCO link is defined as a symmetric, point-to-point link between the master and the slave.
- The SCO link can be thought to be a circuit-switched connection.
- The master can support up to 3 SCO links to the same slave or different slaves.
- The master sends SCO packets in the regular interval known as *Tsco* in the master-to-slave slots.



Physical Links (Cont. 2)

- ACL link is a point-to-multipoint link between the master and all the slaves participating in the piconet.
- The master can establish an ACL link on the per-slot basis with any slave.
- ACL links provide a packet-switched connection.

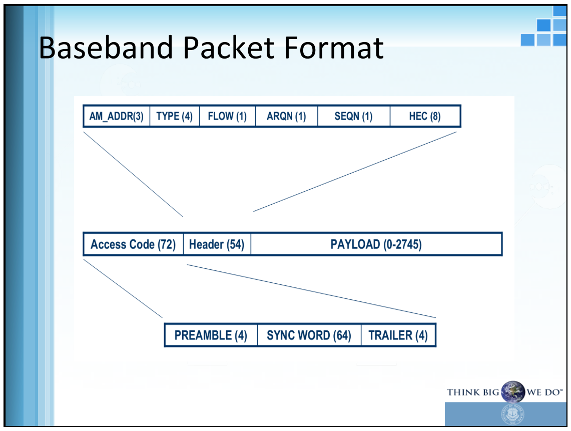


Baseband Specification

Defines many fundamental operations between devices

- Channel Control
- Packet Formats
- Error Corrections
- BT Addressing
- Connections

APPLICATIONS
TCP/IP
HIC
RFCOMM
AUDIO
DATA
CONTROL
L2CAP
LINK MANAGER
Baseband
BASEBAND
RADIO

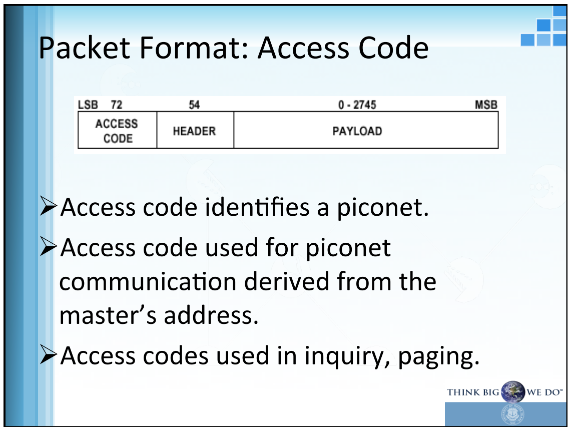


Baseband Packet Format

AM_ADDR(3)	TYPE (4)	FLOW (1)	ARQN (1)	SEQN (1)	HEC (8)

Access Code (72)	Header (54)	PAYLOAD (0-2745)

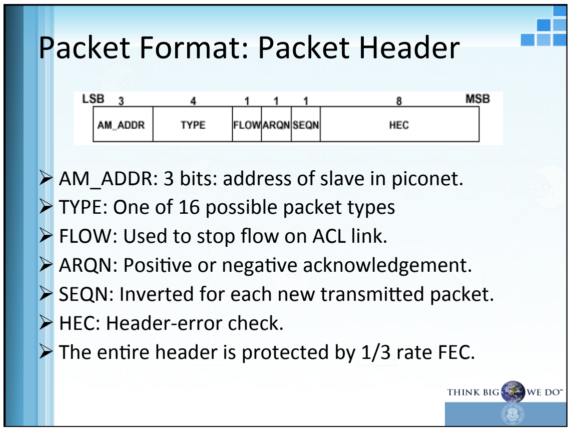
PREAMBLE (4)	SYNC WORD (64)	TRAILER (4)



Packet Format: Access Code

LSB 72	54	0 - 2745 MSB
ACCESS CODE	HEADER	PAYLOAD

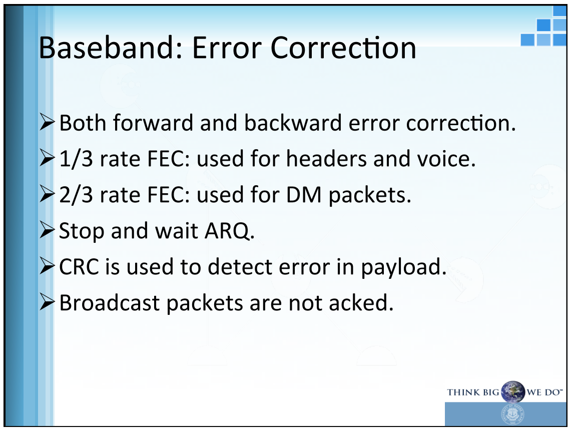
- Access code identifies a piconet.
- Access code used for piconet communication derived from the master's address.
- Access codes used in inquiry, paging.



Packet Format: Packet Header

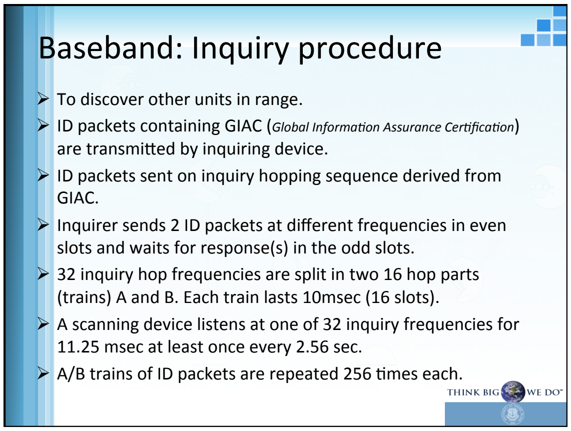
LSB 3	4	1	1	1	8 MSB
AM_ADDR	TYPE	FLOW	ARQN	SEQN	HEC

- AM_ADDR: 3 bits: address of slave in piconet.
- TYPE: One of 16 possible packet types
- FLOW: Used to stop flow on ACL link.
- ARQN: Positive or negative acknowledgement.
- SEQN: Inverted for each new transmitted packet.
- HEC: Header-error check.
- The entire header is protected by 1/3 rate FEC.



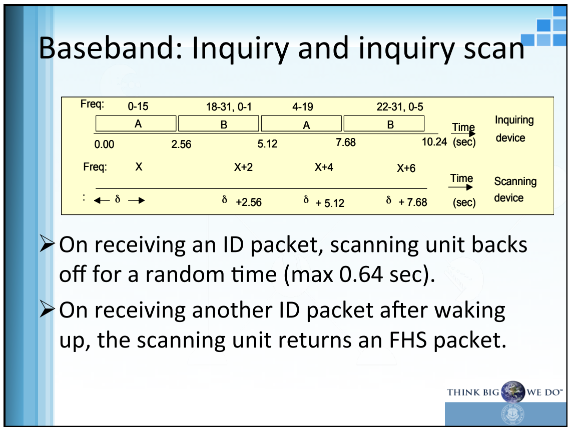
Baseband: Error Correction

- Both forward and backward error correction.
- 1/3 rate FEC: used for headers and voice.
- 2/3 rate FEC: used for DM packets.
- Stop and wait ARQ.
- CRC is used to detect error in payload.
- Broadcast packets are not acked.



Baseband: Inquiry procedure

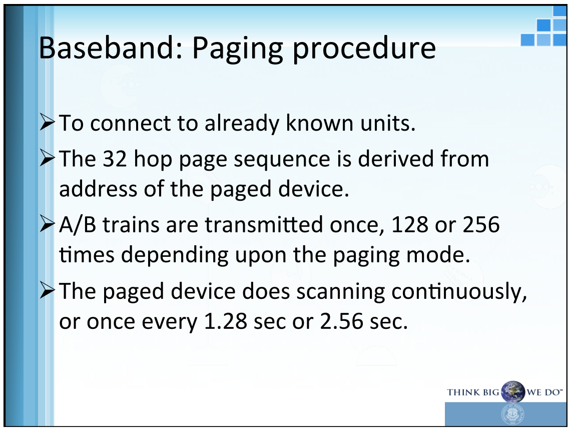
- To discover other units in range.
- ID packets containing GIAC (*Global Information Assurance Certification*) are transmitted by inquiring device.
- ID packets sent on inquiry hopping sequence derived from GIAC.
- Inquirer sends 2 ID packets at different frequencies in even slots and waits for response(s) in the odd slots.
- 32 inquiry hop frequencies are split in two 16 hop parts (trains) A and B. Each train lasts 10msec (16 slots).
- A scanning device listens at one of 32 inquiry frequencies for 11.25 msec at least once every 2.56 sec.
- A/B trains of ID packets are repeated 256 times each.



Baseband: Inquiry and inquiry scan

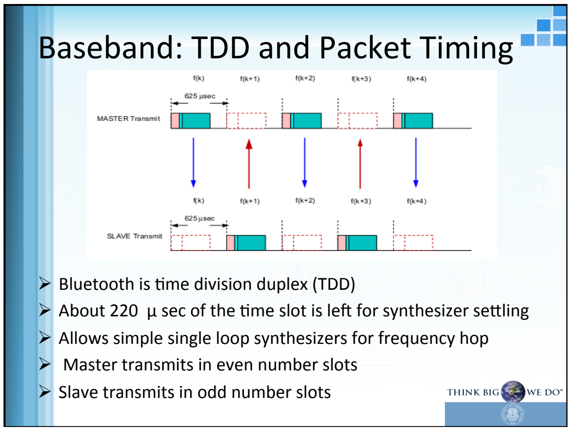
Freq:
0-15
18-31, 0-1
4-19
22-31, 0-5
A
B
A
B
Time (sec)
Inquiring device
0.00
2.56
5.12
7.68
10.24
Freq:
X
X+2
X+4
X+6
Time (sec)
Scanning device
δ
δ +2.56
δ + 5.12
δ + 7.68

- On receiving an ID packet, scanning unit backs off for a random time (max 0.64 sec).
- On receiving another ID packet after waking up, the scanning unit returns an FHS packet.



Baseband: Paging procedure

- To connect to already known units.
- The 32 hop page sequence is derived from address of the paged device.
- A/B trains are transmitted once, 128 or 256 times depending upon the paging mode.
- The paged device does scanning continuously, or once every 1.28 sec or 2.56 sec.



Baseband: TDD and Packet Timing

f(k)
f(k+1)
f(k+2)
f(k+3)
f(k+4)
625 µsec
MASTER Transmit
f(k)
f(k+1)
f(k+2)
f(k+3)
f(k+4)
625 µsec
SLAVE Transmit

- Bluetooth is time division duplex (TDD)
- About 220 µ sec of the time slot is left for synthesizer settling
- Allows simple single loop synthesizers for frequency hop
- Master transmits in even number slots
- Slave transmits in odd number slots

Baseband: Connection state

- Active mode:
  - Bluetooth unit listens for each master transmission.
  - Slaves not addressed can sleep through a transmission.
  - Periodic master transmissions used for sync.
- Sniff mode:
  - Unit does not listen to every master transmission.
  - Master polls such slaves in specified sniff slots.

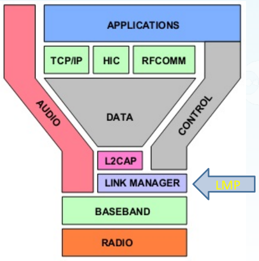
Baseband: Connection state

- Hold mode
  - Master and slave agree on a time duration for which the slave is not polled.
  - Typically used for scanning, paging, inquiry or by bridging slaves to attend to other piconets.
- Park mode
  - Slave gives up AM_ADDR.
  - Listens periodically for a beacon transmission to synchronize and uses PM_ADDR/AR_ADDR for unparking.

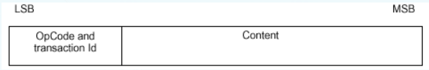
Link Management Protocol

Set up and Manage Baseband Connections

- Piconet Mgmt.
- Security
- Power Mgmt.
- Link Configuration

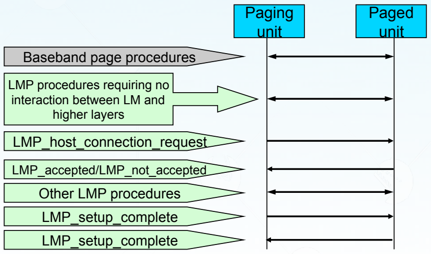


Link Manager Protocol (LMP)



- Used for link set-up, security and control.
- All LMP messages are single slot packets.
- Priority higher than user data (L2CAP).
- Payload body for LM PDUs:

LMP: Connection Establishment

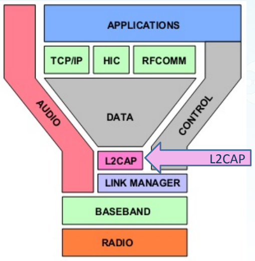


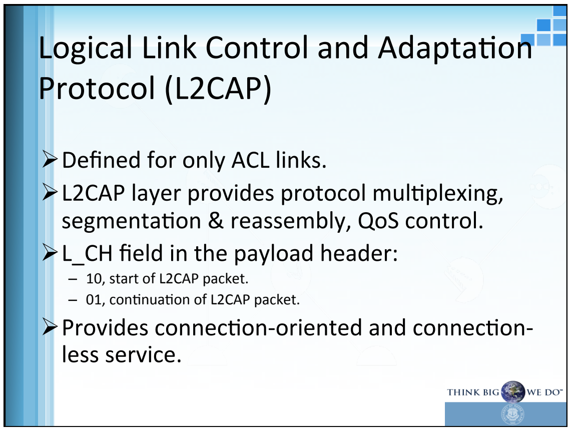
Paging unit
Paged unit
Baseband page procedures
LMP procedures requiring no interaction between LM and higher layers
LMP_host_connection_request
LMP_accepted/LMP_not_accepted
Other LMP procedures
LMP_setup_complete
LMP_setup_complete

L2CAP

Logical Link Control and Adaptation Protocol

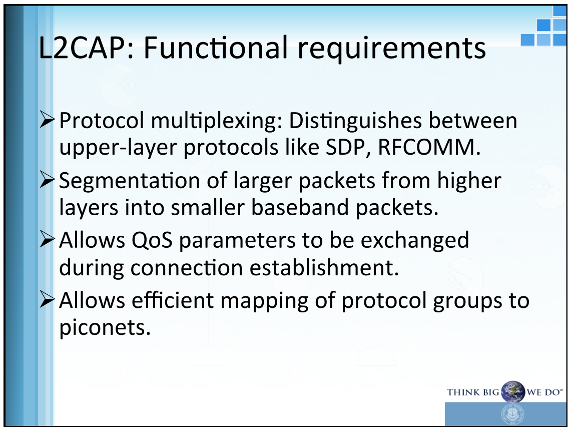
- Protocol Multiplexing
- Segmentation and Reassembly of up to 64 Kbyte packets
- Quality of Service Negotiation





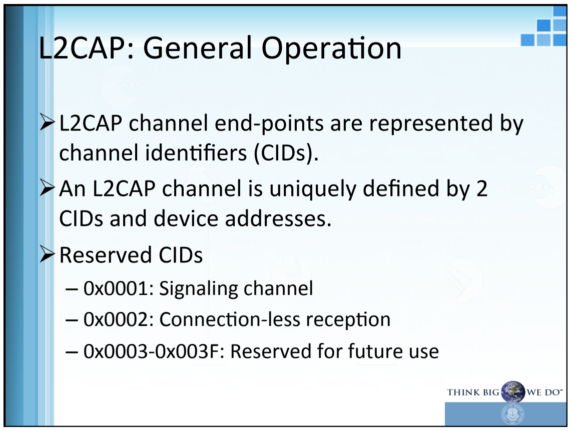
Logical Link Control and Adaptation Protocol (L2CAP)

- Defined for only ACL links.
- L2CAP layer provides protocol multiplexing, segmentation & reassembly, QoS control.
- L_CH field in the payload header:
  - 10, start of L2CAP packet.
  - 01, continuation of L2CAP packet.
- Provides connection-oriented and connection-less service.



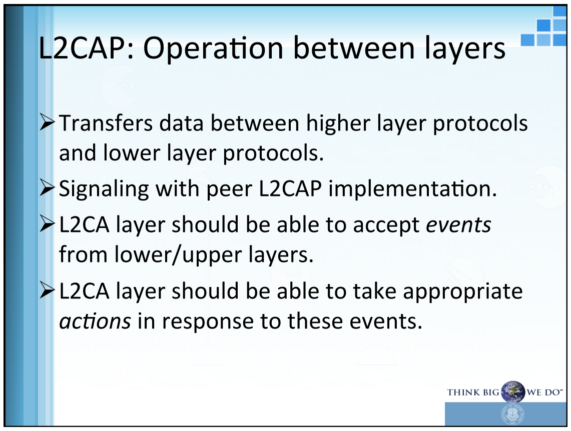
L2CAP: Functional requirements

- Protocol multiplexing: Distinguishes between upper-layer protocols like SDP, RFCOMM.
- Segmentation of larger packets from higher layers into smaller baseband packets.
- Allows QoS parameters to be exchanged during connection establishment.
- Allows efficient mapping of protocol groups to piconets.



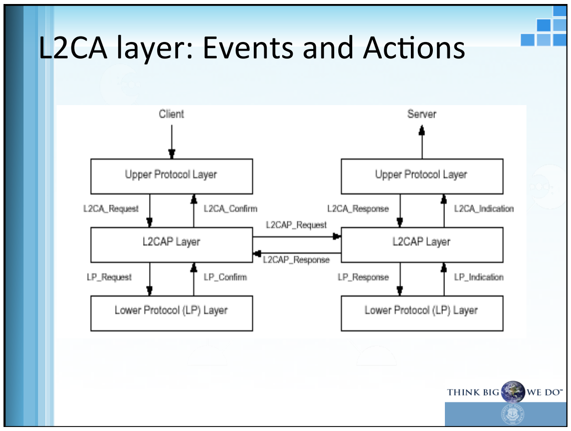
L2CAP: General Operation

- L2CAP channel end-points are represented by channel identifiers (CIDs).
- An L2CAP channel is uniquely defined by 2 CIDs and device addresses.
- Reserved CIDs
  - 0x0001: Signaling channel
  - 0x0002: Connection-less reception
  - 0x0003-0x003F: Reserved for future use

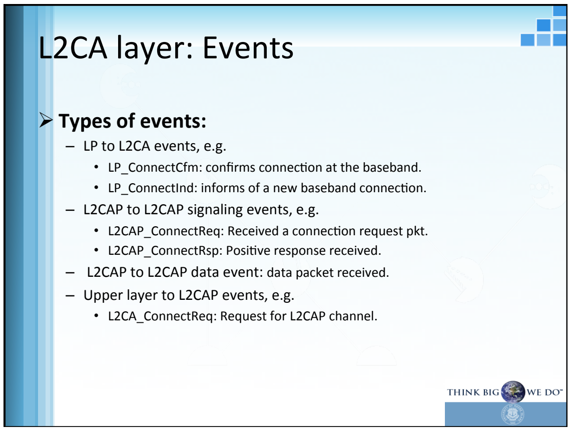


L2CAP: Operation between layers

- Transfers data between higher layer protocols and lower layer protocols.
- Signaling with peer L2CAP implementation.
- L2CA layer should be able to accept *events* from lower/upper layers.
- L2CA layer should be able to take appropriate *actions* in response to these events.

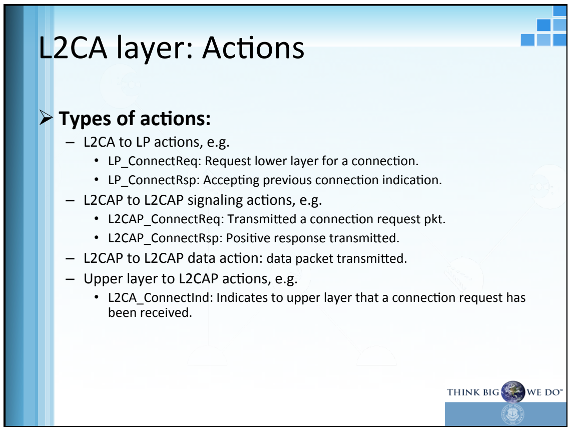


L2CA layer: Events and Actions



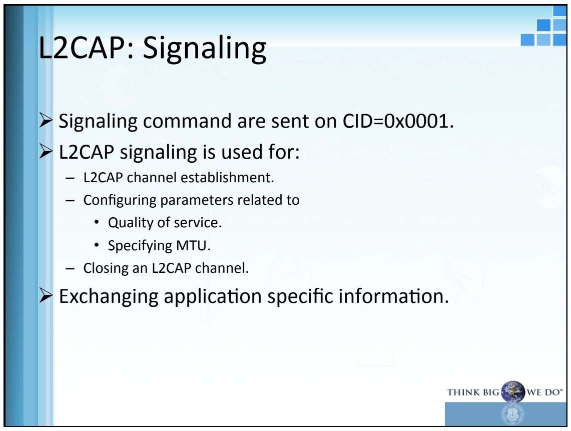
L2CA layer: Events

- **Types of events:**
  - LP to L2CA events, e.g.
    - LP_ConnectCfm: confirms connection at the baseband.
    - LP_ConnectInd: informs of a new baseband connection.
  - L2CAP to L2CAP signaling events, e.g.
    - L2CAP_ConnectReq: Received a connection request pkt.
    - L2CAP_ConnectRsp: Positive response received.
  - L2CAP to L2CAP data event: data packet received.
  - Upper layer to L2CAP events, e.g.
    - L2CA_ConnectReq: Request for L2CAP channel.



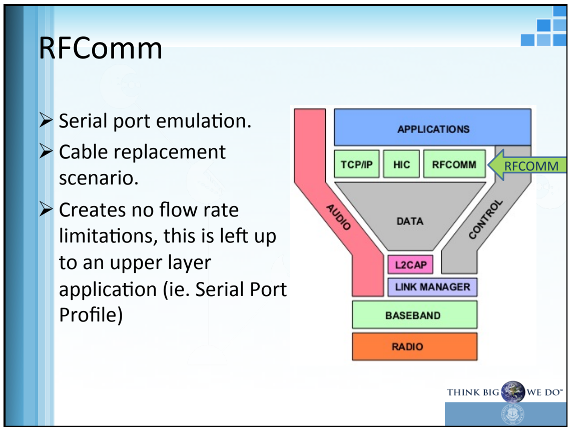
L2CA layer: Actions

- **Types of actions:**
  - – L2CA to LP actions, e.g.
    - LP_ConnectReq: Request lower layer for a connection.
    - LP_ConnectRsp: Accepting previous connection indication.
  - – L2CAP to L2CAP signaling actions, e.g.
    - L2CAP_ConnectReq: Transmitted a connection request pkt.
    - L2CAP_ConnectRsp: Positive response transmitted.
  - – L2CAP to L2CAP data action: data packet transmitted.
  - – Upper layer to L2CAP actions, e.g.
    - L2CA_ConnectInd: Indicates to upper layer that a connection request has been received.



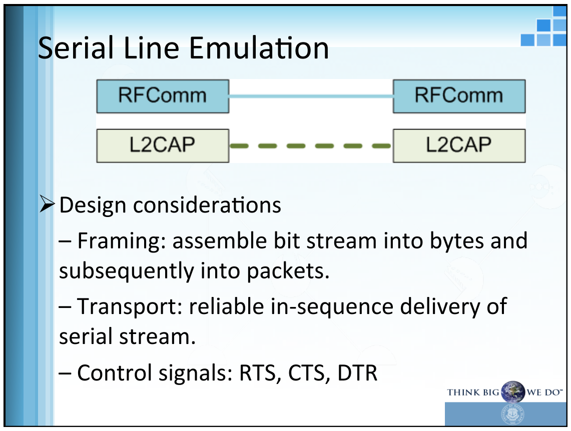
L2CAP: Signaling

- Signaling command are sent on CID=0x0001.
- L2CAP signaling is used for:
  - – L2CAP channel establishment.
  - – Configuring parameters related to
    - Quality of service.
    - Specifying MTU.
  - – Closing an L2CAP channel.
- Exchanging application specific information.



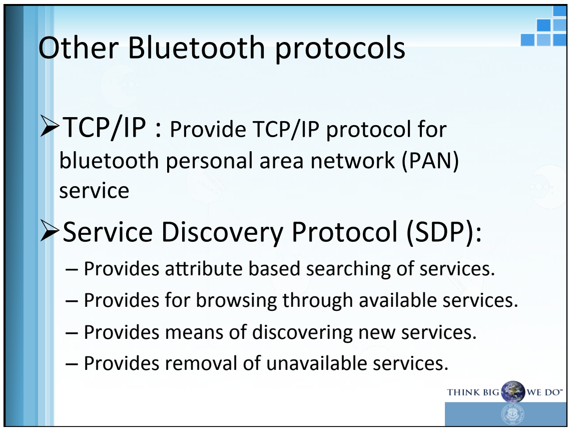
RFComm

- Serial port emulation.
- Cable replacement scenario.
- Creates no flow rate limitations, this is left up to an upper layer application (ie. Serial Port Profile)



Serial Line Emulation

- Design considerations
  - – Framing: assemble bit stream into bytes and subsequently into packets.
  - – Transport: reliable in-sequence delivery of serial stream.
  - – Control signals: RTS, CTS, DTR



Other Bluetooth protocols

- TCP/IP : Provide TCP/IP protocol for bluetooth personal area network (PAN) service
- Service Discovery Protocol (SDP):
  - – Provides attribute based searching of services.
  - – Provides for browsing through available services.
  - – Provides means of discovering new services.
  - – Provides removal of unavailable services.