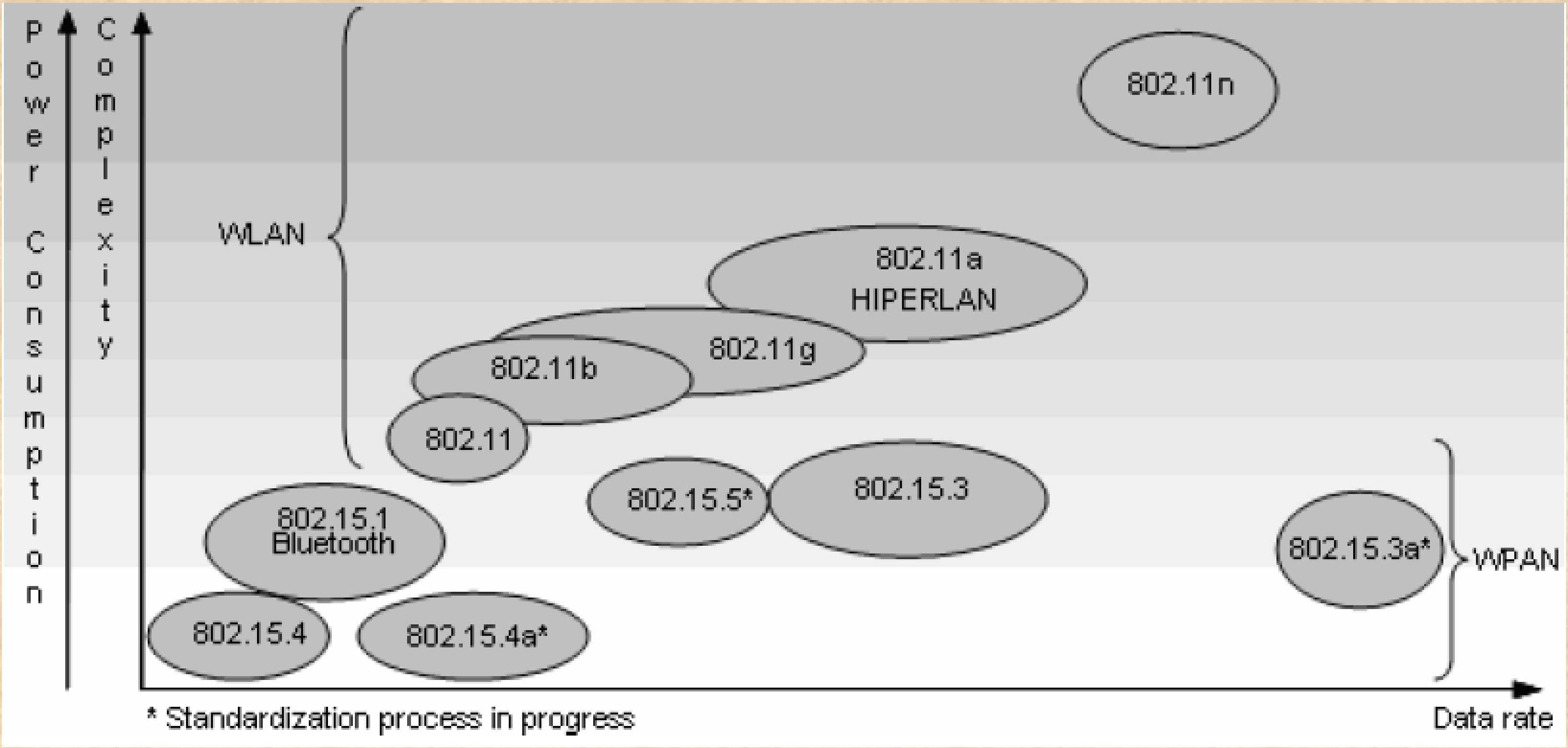
Topic 2: Wireless PANs

- Introduction
- Why Wireless PANs
- The Bluetooth Technology
  - History and Applications
  - Technical Overview
  - The Bluetooth Specifications
  - Piconet Synchronization and Bluetooth Clocks
  - Master-Slave Switch
  - Bluetooth Security
- Enhancements to Bluetooth
  - Bluetooth Interference Issues
  - Intra and Inter Piconet Scheduling
  - Bridge Selection
  - Traffic Engineering
  - QoS and Dynamic Slot Assignment
  - Scatternet Formation
- The IEEE 802.15 Working Group for WPANs
  - The IEEE 802.15.3
  - The IEEE 802.15.4
- Comparison between WPAN Systems
  - Range
  - Data Rate
  - Support for Voice
  - Support for LAN Integration
  - Power Management
  - Comparison and Summary of Results
- WLANs versus WPANs
- Conclusion and Future Directions

Introduction

- WPANs are short to very-short range wireless networks (from a couple centimeters to a couple of meters)
- WPANs can be used to replace cables between computers and their peripherals
- The IEEE 802 has established the IEEE 802.15 WG for WPANs, which standardizes protocols and interfaces for WPANs
- The best example representing WPANs is the industry standard Bluetooth, which can be found in many consumer electronics
- Other less popular examples of WPAN technologies include Spike, IrDA and in the broad sense HomeRF

WLAN and WPAN Standards



Note: As of March 2006, the 802.15.3a task group has been officially withdrawn from the IEEE

Operating space of the various IEEE 802 WLAN and WPAN standards and other activities still in progress

Why Wireless PANs

- **WPAN should allow devices to create or provide data/voice access points, personal ad hoc connectivity, and a replacement for connecting cables**
- **The operating range for these devices is within a personal operating space (POS) of up to 10 meters in all directions, and envelops a stationary or a mobile person**
- **The concept of a POS can also be extended to devices such as printers, scanners, digital cameras, microwave ovens, TVs or VCRs**
- **WPAN systems are expected to provide secure modes of operation, allowing groups of personal devices to interconnect while excluding connectivity to other non-essentials**
- **As WPANs use the license-free radio frequencies (e.g., ISM band), they have to coexist with other RF technologies that make use of these frequencies**

The Bluetooth Technology

- **Bluetooth (BT) has been a topic of considerable buzz in the telecommunications industry for the past few years**
- **Bluetooth is named after a 10th-century Viking king known for his success in uniting Denmark and Norway during his rule around 960 AD**
- **Bluetooth is a low cost and short-range radio communication standard that was introduced as an idea in Ericsson Laboratories back in 1994**
- **Engineers envisioned a need for a wireless transmission technology that would be cheap, robust, flexible, and consume low power**
- **Bluetooth was chosen to serve as the baseline of the IEEE 802.15.1 standard for WPANs, which can support both synchronous traffic such as voice, and asynchronous data communication**

Applications of Bluetooth

Some application areas where Bluetooth networks could be explored

- **Consumer – Wireless PC peripherals, smart house wireless PC peripherals, smart house integration, etc.**
- **Games – Controllers, virtual reality, iPODs, etc.**
- **Professional – Pagers, PDAs, cell phones, desktops, automobiles, etc.**
- **Services – Shipping, travel, hotels, etc.**
- **Industry – Delivery (e.g., scanners, printers), assembly lines, inspections, inventory control, etc.**
- **Sports training – Health sensors, monitors, motion tracking, etc.**
- **Military – Combat and maintenance**

Bluetooth – Technical Overview

- **The Bluetooth Specification (version 1.1) describes radio devices designed to operate over very short ranges (in the order of 10 meters) or optionally a medium range (100 meters) radio link capable of voice or data transmission to a maximum capacity of 720 kbps per channel (with a nominal throughput of 1 Mbps)**

- **Radio frequency operation is in the unlicensed ISM band at 2.4 to 2.48 GHz, using a frequency hopping spread spectrum (FHSS), full-duplex signal at up to 1600 hops/seconds, hopping among 79 frequencies at 1 MHz intervals**
- **RF output is 0 dBm (1 mW) in the 10m range and -30 to +20 dBm (100 mW) in longer ranges.**
- **Has three low power states – PARK, HOLD, and SNIFF – and a normal power state when the device is transmitting, while the power savings varies due to the reduced transmit-receive duty cycle**

- **The Bluetooth specifications are divided into two parts:**
  - ***The Core* – This portion specifies components such as the radio, base band (medium access), link manager, service discovery protocol, transport layer, and interoperability with different communication protocols**
  - ***The Profile* – The Profile portion specifies the protocols and procedures required for different types of Bluetooth applications**

Bluetooth – Technical Overview

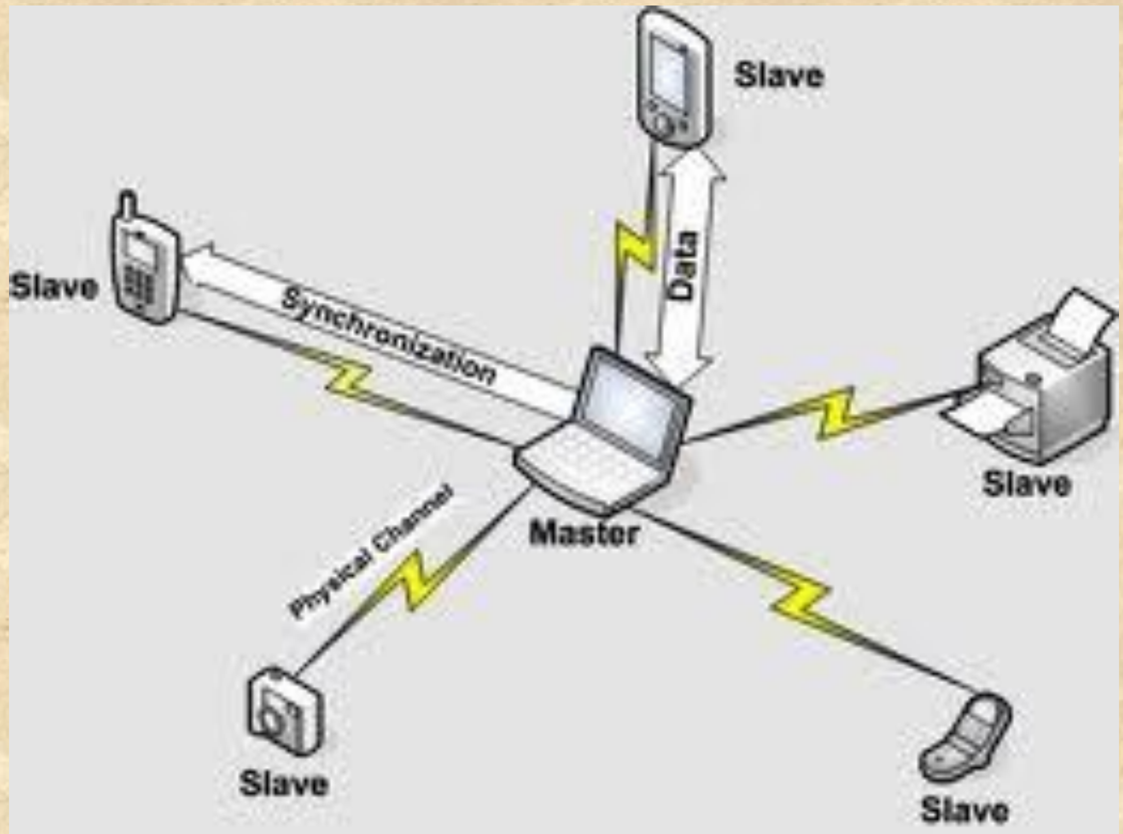
- **Whenever a pair or small group of Bluetooth devices come within radio range of each other, they can form an ad hoc network without requiring any infrastructure**

- **Devices are added or removed from the network dynamically and they can connect to or disconnect from an existing network at will and without interruption to the other participants**

- **In Bluetooth, the device taking the initiative to start communication to another device assumes the role of a *master*, while the recipient becomes a *slave***

- **The basic architectural unit of a Bluetooth is a *Piconet*, composed of one master device and up to seven active *slave devices*, which can communicate with each other only through the master**

Bluetooth Piconet



An example of a Piconet

Bluetooth – Technical Overview

- **Every Bluetooth device is exactly the same except for a 48-bit device identifier (BD_ADDR)**
- **Beside up to 7 active slaves, additional devices can be connected to a Piconet in a *parked* state in which they listen but do not participate**
- **When they want to participate, they are swapped in and one of the active devices is swapped out**
- **If the acting master leaves the Piconet, one of the slaves assumes its role**
- **With this method, up to 255 devices can be virtually connected to the Piconet**
- **Also, each piconet uses a different Frequency Hopping Sequence (FHS) in order to reduce interference with other nearby piconets**
- **To increase the number of devices in the network, a *scatternet* architecture consisting of several piconets has been proposed**

Bluetooth – Technical Overview

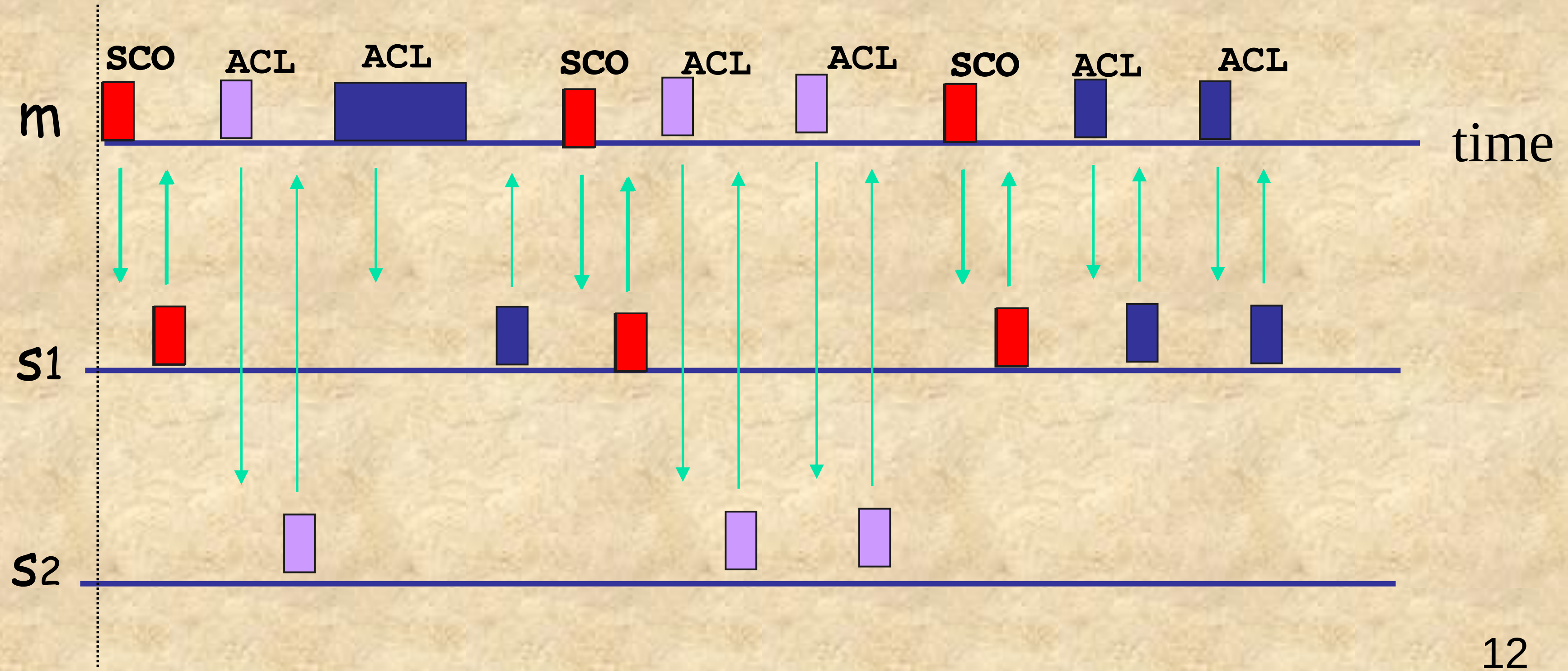
- The Bluetooth specification defines two different types of links for data and voice applications:

- The Synchronous Connection Oriented (SCO) link
  - Symmetric, point-to-point link between the master and one slave
  - Usually used for audio applications with strict Quality of Service (QoS) requirements
    - Master reserves slots for SCO links and can be treated as a circuit switched network
    - SCO traffic is transmitted at predefined regular intervals
    - A voice channel supports a 64 Kbps synchronous simplex channel
    - A piconet supports up to 3 SCO links

- The Asynchronous Connectionless (ACL) link
  - ACL link is treated as a packet switched, point to point and point to multipoint data traffic link
  - The Master maintains one ACL link with each active slave over which upper layer connection can be established and re-transmission is employed only when it is necessary to ensure data integrity

Physical Link Types

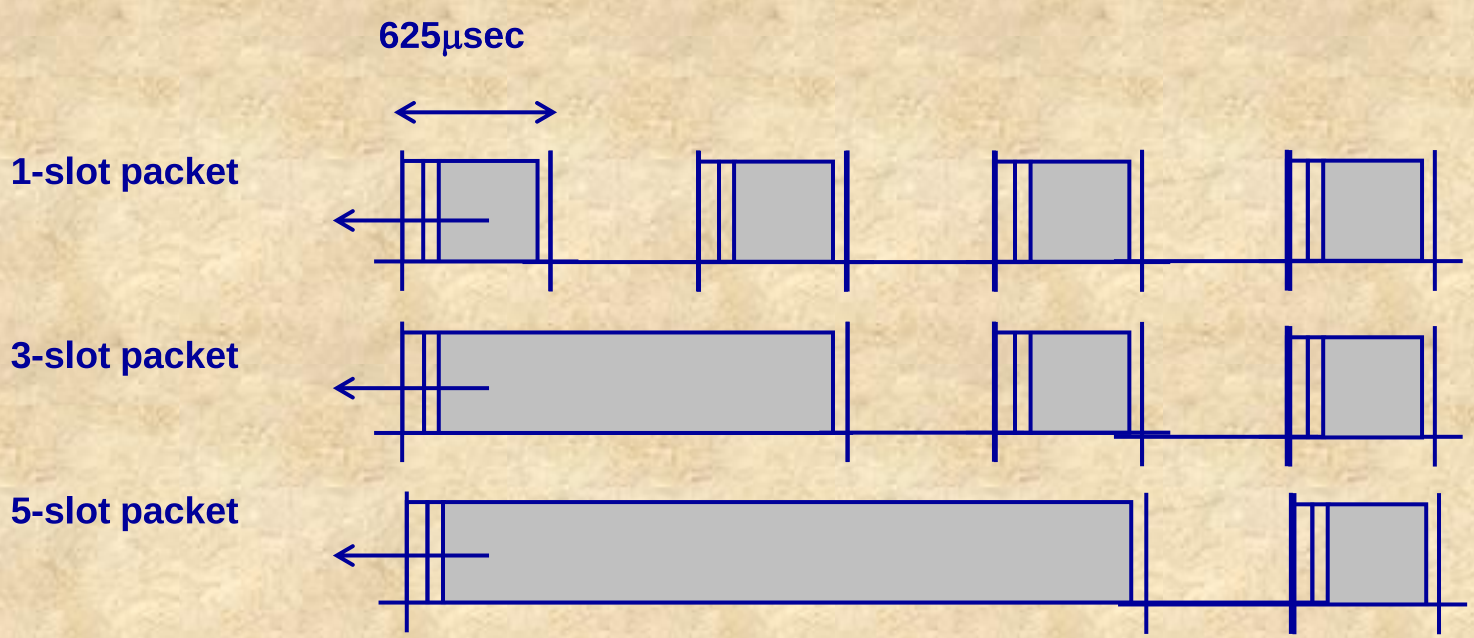
- Synchronous Connection Oriented (SCO) Link
  - Slot reservation at fixed intervals
- Asynchronous Connection-less (ACL) Link
  - Polling access method



Packet transmission in Bluetooth

- **Bluetooth defines a set of packets types, and information can travel in these packet types only**

- **Bluetooth allows the use of 1, 3 and 5 slot packets as depicted below**



Packet transmission in Bluetooth

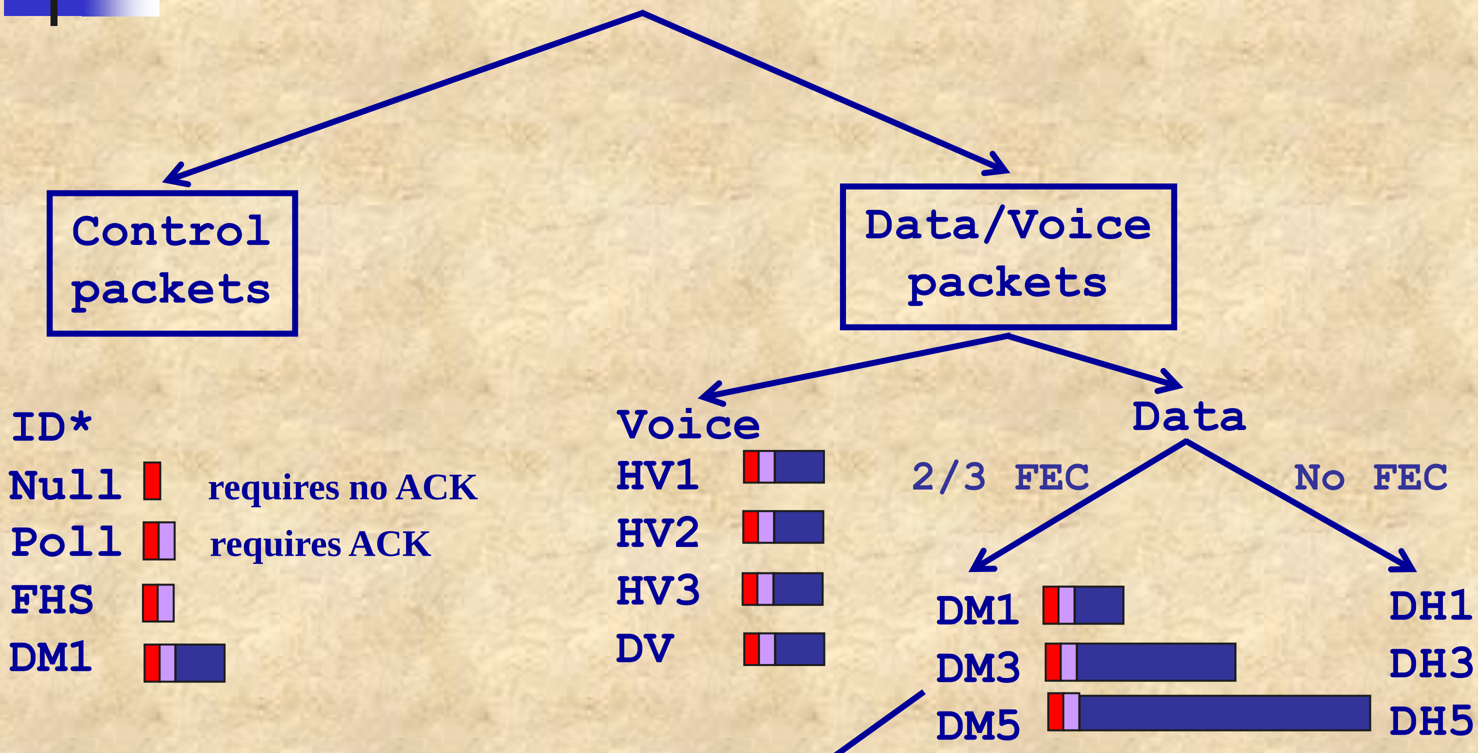
- A TDD scheme divides the channel into 625 μsec slots at a 1 Mb/s rate
- As a result, at most 625 bits can be transmitted in a single slot
- However, to change the Bluetooth device from transmit state to receive state and tune to the next frequency hop, a 259 μsec *turn around time* is kept at the end of the last slot occupied by the packet
- This results in reduction of effective bandwidth available for data transfer
- Bluetooth employs
  - HVx (High-quality Voice) packets for SCO transmissions
  - DMx (Data Medium-rate) packets for ACL data transmissions
  - DHx (Data High-rate) packets for ACL data transmissions
    - x = 1, 3, or 5

Bluetooth packet types

Type	User Payload (bytes)	FEC	Symmetric (Kbps)	Assymetric (Kbps)	Assymetric (kbps)
DM1	0-17	Yes	108.0	108.0	108.0
DH1	0-27	No	172.8	172.8	172.8
DM3	0-121	Yes	256.0	384.0	54.4
DH3	0-183	No	384.0	576.0	86.4
DM5	0-224	Yes	286.7	477.8	36.3
DH5	0-339	No	432.6	721.0	57.6
HV1	0-10	Yes	64.0	-	-
HV3	0-20	Yes	128.0	-	-
HV5	0-30	No	192.0	-	-

- DH: Data high rate; DM: Data medium rate; HV: High Quality voice
- Numerical digit indicates the number of 625μs time slots occupied
- Considering its nominal 1 Mbps Piconet bandwidth and the 64 Kbps requirement for a SCO connection, it will be clear later that a Bluetooth Piconet can support up to three simplex SCO links (when using HV3 packets) so as to meet the required QoS needs
  - Q1: why do we speak of a Piconet bandwidth?
  - Q2: how did we reach the max of 3 SCOs?

Packet Types and Bandwidth



Symmetric	Asymmetric	
108.8	108.8	108.8
258.1	387.2	54.4
286.7	477.8	36.3

Symmetric	Asymmetric	
172.8	172.8	172.8
390.4	585.6	86.4
433.9	723.2	57.6

Connection Setup in Bluetooth

- Connection setup in Bluetooth starts with each node discovering its neighbors, a process that is called *inquiry*

- For two devices to discover each other, while one of them is in INQUIRY state, the other has to be in INQUIRY SCAN
  - The node in INQUIRY SCAN responds to the INQUIRY of the other node
  - This way the node in INQUIRY state notices the presence of the node in INQUIRY SCAN
- When the devices want to build up a connection, they begin the *page* procedure
- Similar to the inquiry phase, there are two states: PAGE and PAGE SCAN
  - When one of the nodes wants to build up a connection to the other node, it enters in the PAGE state and when the other node enters PAGE SCAN state, the connection setup is concluded
- Q: Who becomes the Master?

Connection Setup in Bluetooth

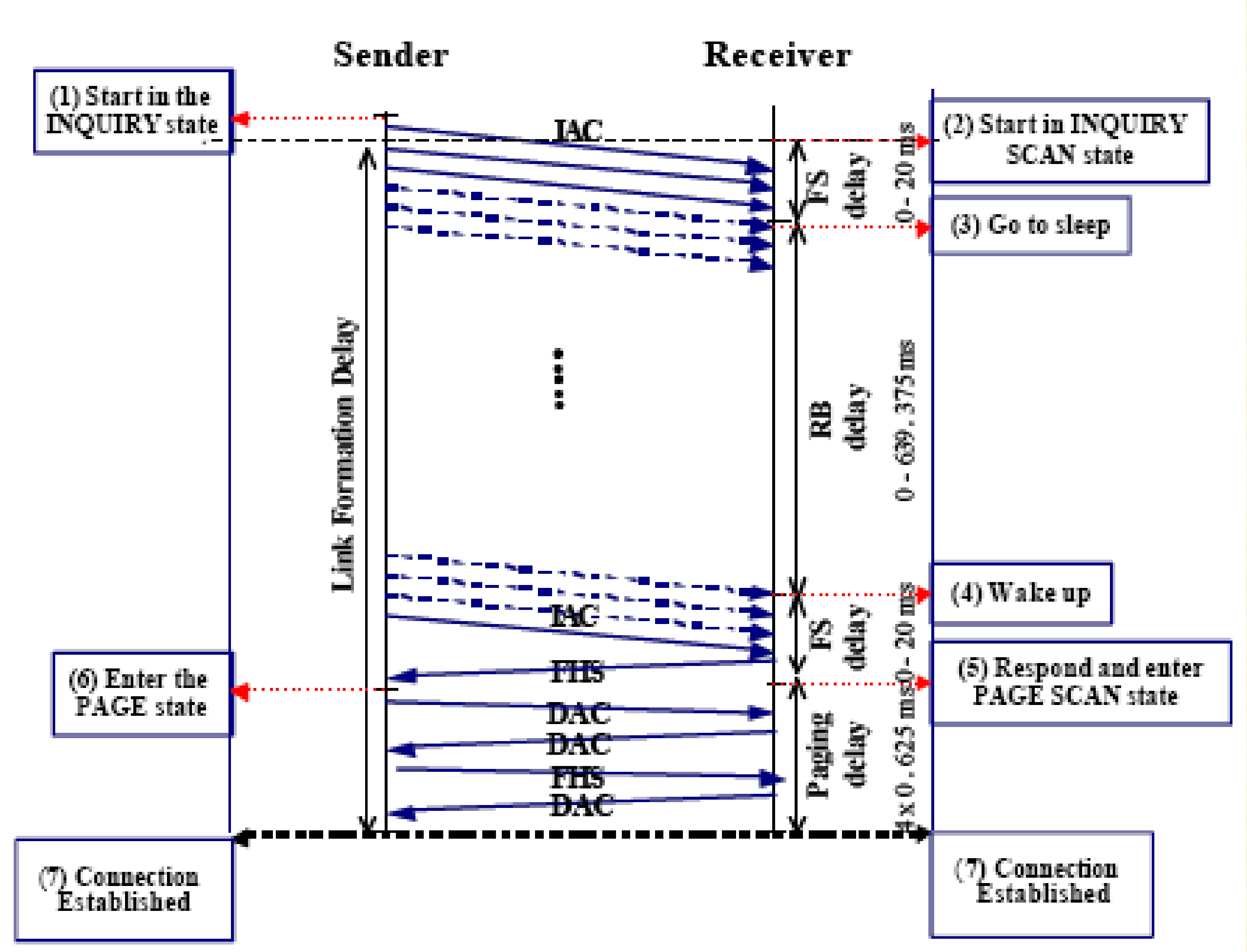
- Pairing usually requires an authentication process where a user must validate the connection between devices.
- The flow of the authentication process varies and usually depends on the interface capabilities of one device or the other.
    - Sometimes pairing is a simple “Just Works” operation, where the click of a button is all it takes to pair (this is common for devices with no UI, like headsets).
    - Other times pairing involves matching 6-digit numeric codes.
    - Older, legacy (v2.0 and earlier), pairing processes involve the entering of a common PIN code on each device. The PIN code can range in length and complexity from four numbers (e.g. “0000” or “1234”) to a 16-character alphanumeric string.

Connection Setup in Bluetooth

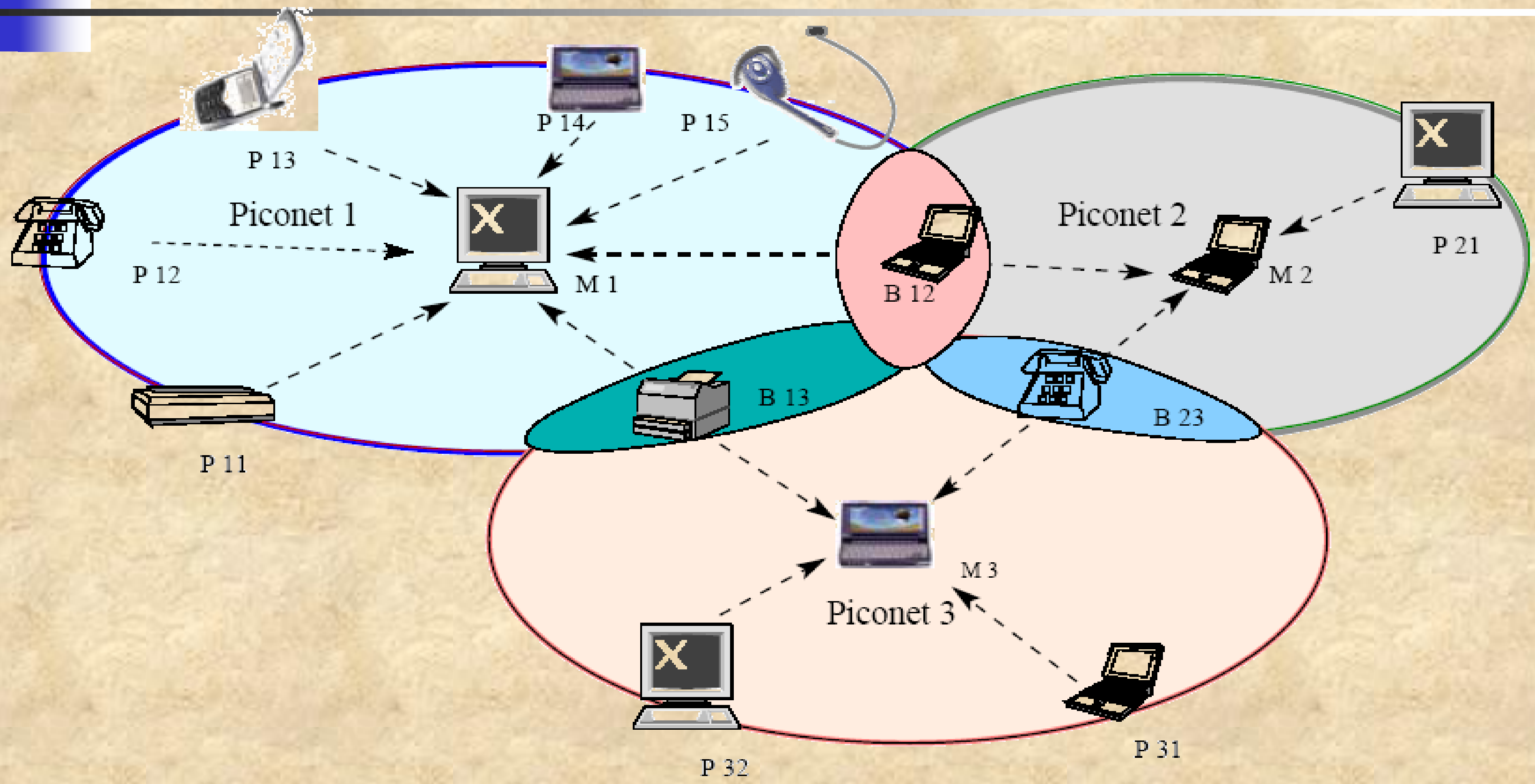
In the inquiry state, nodes use a universal FH sequence

IAC: Inquiry Access Code (broadcast)

DAC: Device Access Code (unicast)



Bluetooth Scatternet



- An example scatternet comprised of three piconets
- Since scatternets span more than a single piconet, a few nodes act as bridges (e.g., B12, B13, B23) responsible for relaying packets across piconet boundaries
- A bridge can only be active in one piconet at a time
- A device can be a slave in more than one piconet but a master in only one piconet
- A bridge needs to synchronize with the Frequency Hopping Sequence (FHS) of the piconet it is communicating with via the Master

Scatternet Formation: Bluetooth Topology Construction Protocol (BTCP)

- Based on a leader election process to control the network formation and ensure that the resulting topology will satisfy the connectivity requirements
- Several properties were imposed as restrictions:
  - A bridge may connect only two piconets
  - The scatternet should consist of the minimum number of piconets
  - The scatternet should be fully connected
  - Two piconets share only one bridge

- BTCP comprises 3 phases
  - PHASE 1: Coordinator election
    - After initialization, the node starts alternating between the INQUIRY and INQUIRY SCAN states
    - Two nodes x and y that discover each other will form a point to point confrontation and compare their VOTES variables (initialized to 1).
    - Node (x) with larger variable is the winner (if equal values are found, node address is the tie breaker)
    - Loser (y) sends FHS packets and votes of the nodes it had won previously to winner, tears down the connection and enters PAGE SCAN $\Rightarrow$ gets eliminated from the election process
    - Winner increases its VOTES by VOTES(y) and resumes election by alternating between INQUIRY and INQUIRY SCAN
    - If there are N nodes, the winner of the N-1st confrontation will be the coordinator and the rest will be in PAGE SCAN

Scatternet Formation: Bluetooth Topology Construction Protocol (BTCP)

- **PHASE 2: Role Determination**
  - **Coordinator has FHS packets (identities + clocks) of all nodes in the network, and knows the total number of nodes, N**
  - **If N < 8, it pages and connects to all nodes (which are in PAGE SCAN state) and forms one piconet, and the coordinator becomes the master**
  - **If N > 7, then more than one piconet must be formed and interconnected via bridge nodes**
  - **If participating nodes impose certain restrictions and criteria (e.g., related to remaining battery life), they can be communicated to coordinator during the election process in addition to the FHS information**
  - **The minimum number of masters P to provide a fully connected scatternet has been proven to be equal to** $P=\left\lceil (17-(289-8N)^{1/2})/2 \right\rceil$, $1 \leq N \leq 36$
  - **The coordinator now selects itself plus P-1 nodes to be designated masters, and P(P-1)/2 as bridges**
  - **The coordinator equally distributed to the designated masters the remaining nodes to be their slaves**
    - **Coordinator forms a temporary piconet with itself being a master and designated masters being slaves (while they are in the PAGE SCAN state)**
    - **Master transmits to each slave its connectivity list**
    - **Master instructs slaves to start PHASE 3, and tears down the temporary piconet**

Scatternet Formation: Bluetooth Topology Construction Protocol (BTCP)

- **PHASE 3: Actual Connection Establishement**
  - **Each master x pages and connects to the slaves and bridges sent to it by the coordinator**
  - **When a node is notified that it is a bridge by a master, it waits until it is paged by another master**
  - **When contacted by two masters, a bridge node sends a CONNECTED notification to both masters**
  - **When a master receives a CONNECTED notification from all its assigned bridges, the protocol terminates**

- **See: UCBT–Bluetooth Simulator for ns-2 (**eecs.ceas.uc.edu/~cdmc/ucbt/**)**

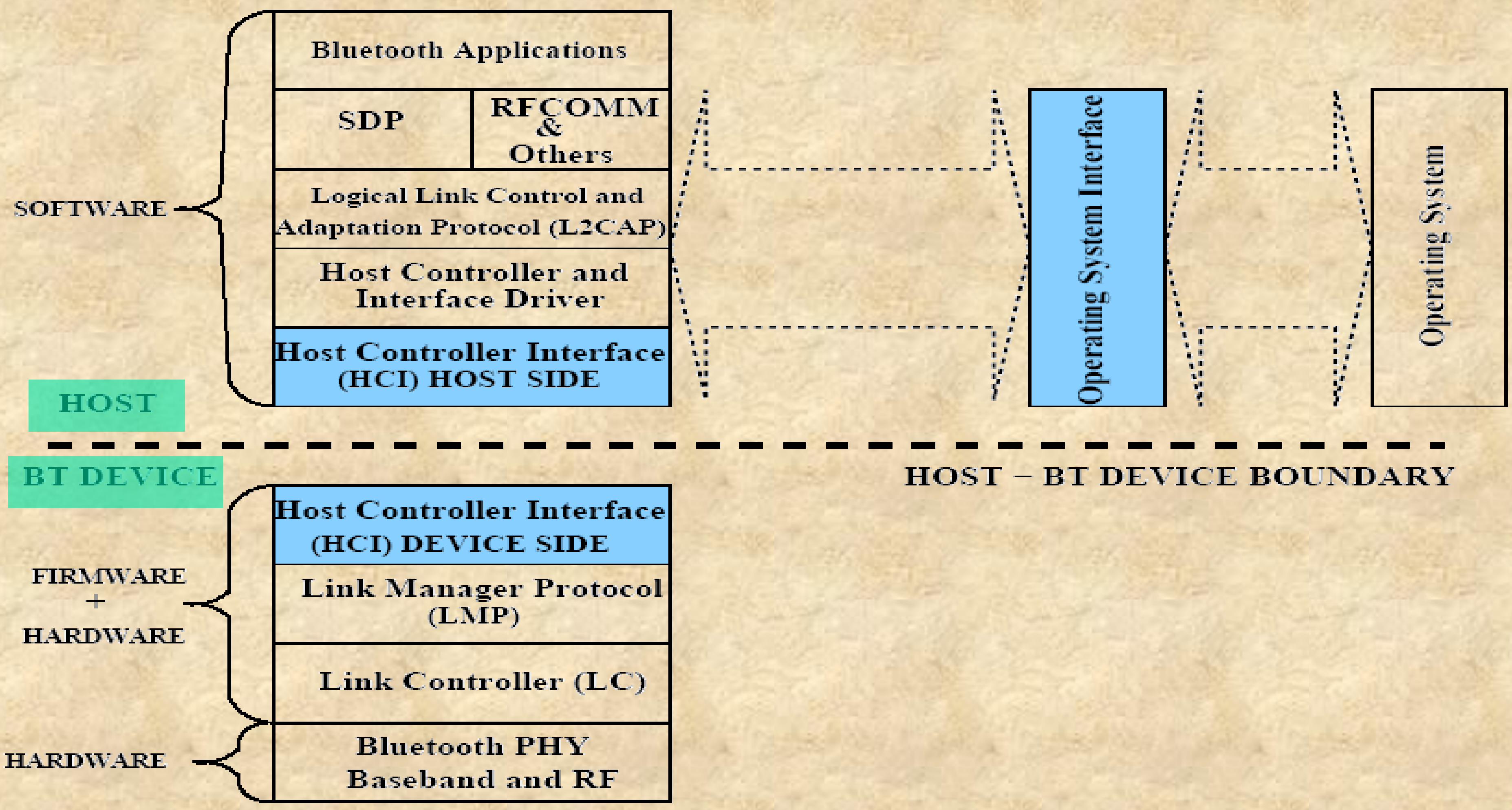
Bluetooth – Specifications

The Bluetooth Specifications include the following

1. The Protocol Stack core functionality
2. The usage Profiles for different applications

- **The protocol stack defines all layers unique to the Bluetooth technology**
- **Bluetooth core Specifications only define the Physical and the Data Link layers of the OSI Protocol Stack**
- **The application layer shown in the figure on the next slide actually includes all the upper layers (IP, Transport, Application) sitting on the RFCOMM and the SDP**
  - **These layers are not themselves part of the stack and are handled in software**
  - **They communicate with lower layers via the Host Controller and the lower layers (RF, Baseband and LMP) are built in hardware modules**

Layered structure of Bluetooth Protocol Stack



Radio Layer

- Responsible for the actual transmitting and receiving of packets of information on the physical channel

- Currently, many other wireless devices operate in this band and, like 802.11b devices
  - Bluetooth mitigates this effect using FHSS and FEC to reduce the impact of noise on long distance links

- Not all Bluetooth devices have the same signal strength nor can cover the same distance. Most of the devices have a freedom in selecting their output power level. The Bluetooth specification sorts devices based on their power class
  - Class 1 min output:1 mW, max output: 100 mW, distance: up to 100 meters
  - Class 2 min output:0.25 mW, max output: 2.5 mW, distance: up to 10 meters
  - Class 3 min output:1 mW, max output: 1 mW, distance: up to 1 meters

- uses a Binary Frequency Shift Keying (BFSK) modulation technique, which represents a binary 1 as a negative frequency deviation

Baseband

- The baseband incorporates the MAC procedures of Bluetooth
  - determines the packet formats, physical-logical channels, and different methods for transferring voice and data
  - provides link set-up and control routines for the layers above
  - provides lower level encryption mechanisms to offer some security to links

Link Control Layer

- **Responsible for the encoding and decoding of Bluetooth packets from the data payload and parameters related to the physical channel, logical transport and logical link**

Link Manager Protocol

- **LMP messages are used for link setup, link control/configuration, power control, and the security aspects like authentication, link-key management, and data encryption**

- **It also provides a mechanism for measuring the QoS and the Received Signal Strength Indication (RSSI)**

- **The link manager provides the functionality to attach/detach slaves, switch roles between a master and a slave, and establish ACL/SCO links**

- **Finally, it handles the low power modes hold, sniff and park, designed to save power when the device has no data to send**

Host Controller Interface

- **The Host Controller Interface (HCI) provides a uniform command interface to the baseband and the LMP layers, and also to the H/W status and the control registers (i.e., it gives higher-level protocols the possibility to access lower layers)**
- **The transparency allows the HCI to be independent of the physical link between the module and the host**
- **The host application uses the HCI interface to send command packets to the Link Manager, such as setting up a connection or starting an inquiry**
- **The HCI itself resides in firmware on the Bluetooth hardware module**
- **It implements the commands for accessing the baseband, the LMP and the hardware registers, as well as for sending messages upward to the host**

Logical Link Control and Adaptation Protocol

- The Logical Link Control and Adaptation Protocol (L2CAP) layer offers a transport protocol and shields the specifics of the lower layers and provides a packet interface to higher layers
- responsible for managing the ordering of submission of PDU fragments to the baseband and scheduling
- At L2CAP level, the concepts of master and slave devices does not exist anymore as it provides a common base for data communication
- Provides a connection oriented and connectionless messaging to upper layer protocols.
- Its features are connection flow control, error detection, and segmentation and reassembly of messages.
- It is built around the concept of *channels*, a notion similar to the TCP ports. Any L2CAP channel is described by a number between the range 1-65535.
- L2CAP can operate in several modes, such as basic, flow control mode, and retransmission mode.
- All the modes deliver unreliable communication similar to UDP except for the retransmission mode.

RFCOMM

- **RFCOMM is a simple transport protocol that provides serial port emulation over the L2CAP protocol, and is intended for cable replacement**
- **Before the retransmission L2CAP mode was introduced, the only way to use a reliable network mode such as TCP was to use the RFCOMM channels.**
- **This protocol is built over the L2CAP protocol and offers an emulation for a serial cable.**
- **It was intended as a wireless replacement for RS-232 serial communication applications and included the control signals.**
- **It offers 20 connection channels, as opposed to 65535 of L2CAP and this made tricky the allocation and usage of the RFCOMM channels.**
- **Despite being a serial communication emulator, it is very often used as a reliable transport layer.**

Service Discovery Protocol (SDP)

- **The Service Discovery Protocol (SDP) is defined to provide Bluetooth entities with methods of finding what services are available from each other**

- **The protocol should be able to determine the properties of any future or present service, of an arbitrary complexity in any operating environment**

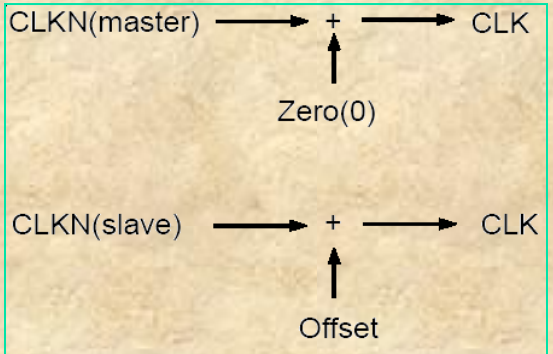
- **A very important part of Bluetooth technology since the range of services available is expected to grow rapidly as developers bring out new products**

Bluetooth Profiles

- **A profile is defined as a combination of protocols and procedures that are used by devices to implement specific services as described in the Bluetooth usage models**
- **For example, the “headset” profile uses AT Commands and the RFCOMM protocol and is one of the profiles used in the “Ultimate Headset” usage model**
- **Profiles are used to maintain interoperability between devices (i.e., all devices conforming to a specific profile will be interoperable), which is one of the Bluetooth’s primary goals**

Piconet Synchronization

- Every Bluetooth unit has an internal clock called the native clock (CLKN), and a Bluetooth clock is derived from this free running native clock
- For synchronization with other units, offsets are added to the native clock to obtain temporary Bluetooth clocks (CLK), which are mutually synchronized
- When a piconet is established, the master's native clock is communicated to all its slaves to generate the offset value
- The Master keeps an exact interval of M*625µsec (where M is an even, positive integer greater than 0) between consecutive transmissions
- The slave's Rx timing is adjusted with every packet sent in the master-to-slave slot, whereas the slave's Tx timing is adjusted based on the most recent slave Rx timing



Bluetooth – Security

- Bluetooth devices use a combination of the Personal Identification Number (PIN) and a Bluetooth address
- Bluetooth addresses are usually represented in hexadecimal colon separated format such as 00:0f:fa:ad:ea:f0. The importance of these addresses in networking is substantial since they are used for device identification in a network.
- Data encryption can be used to further enhance the degree of Bluetooth security
- FHSS alleviates interference as the radio hops between the channels at a fast speed of 1600 hops per second which provides some level of security on data transmission
- However, this hopping procedure does not add any security on the link, since the hopping sequence is broadcasted in clear at the initiation of a connection.
- In addition, the low power transmissions prevent the radio signals from propagating too far
- Only the information in a Bluetooth packet payload is encrypted

Conclusions and Future Directions

- **Wireless PANs are also experiencing a considerable growth, but clearly not as much as the explosive growth seen in the wireless LANs arena**
- **Obviously, this is largely due that wireless PANs are much more recent than wireless LANs**
- **Nevertheless, the vast availability of Bluetooth devices and the standardization of IEEE of various WPAN systems will take this field to a new level**
- **There are numerous environments where WPANs are very suitable such as in sensor networks, while in the home and in the office, WPANs will be part of our lives**