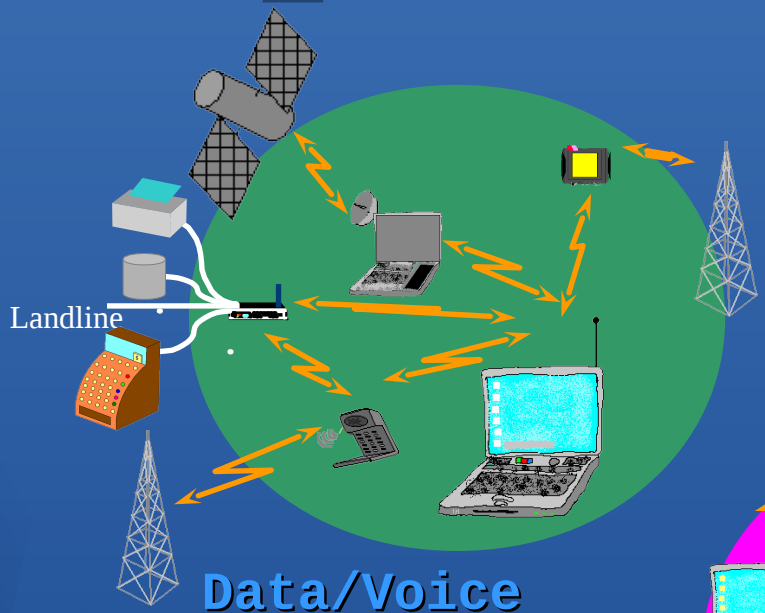
BLUETOOTH

Some slides obtained from: Spanakis Manolis, Computer Science Department CS-532

Who is Bluetooth?

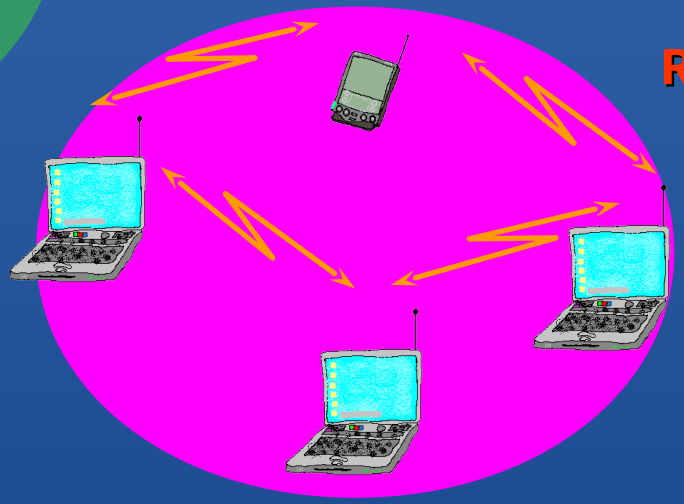
- Harald Blaatand “Bluetooth” II
  - King of Denmark 940-981 AC
- This is one of two Runic stones erected in his capital city of Jelling
  - The stone’s inscription (“runes”) says:
    - Harald christianized the Danes
    - Harald controlled the Danes
    - Harald believes that devices shall seamlessly communicate [wirelessly]

What does Bluetooth do for you?



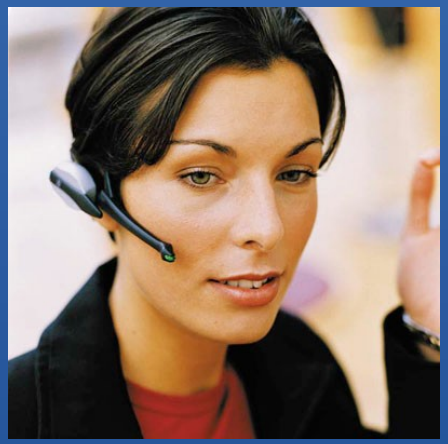
Data/Voice
Access Points

Cable
Replacement

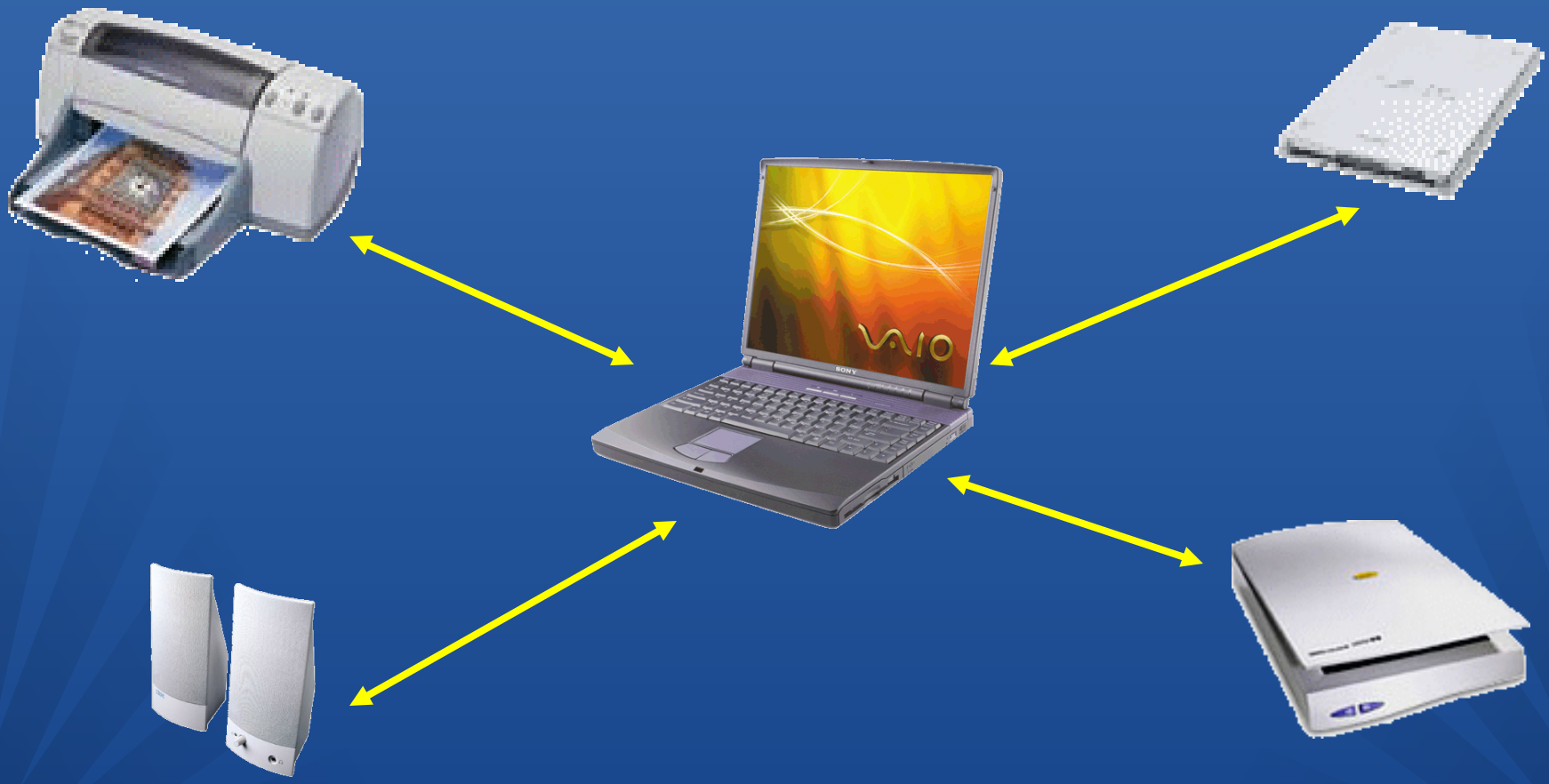


Personal Ad-hoc
Networks

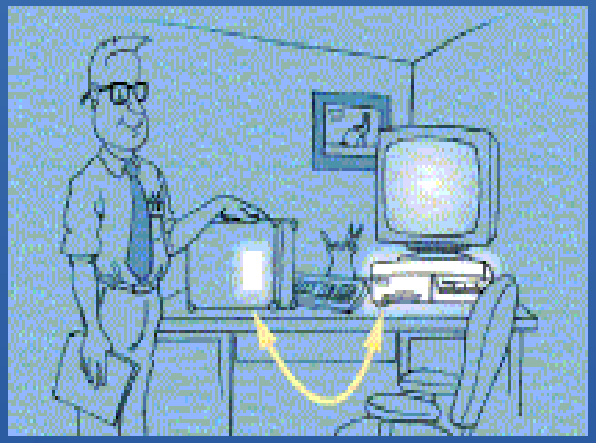
Ultimate Headset



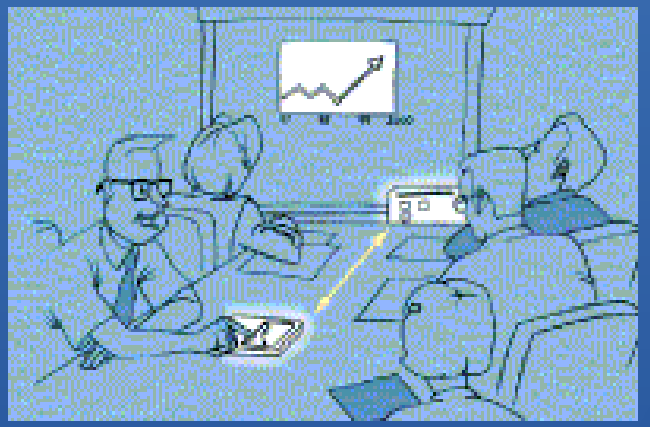
Cordless Computer

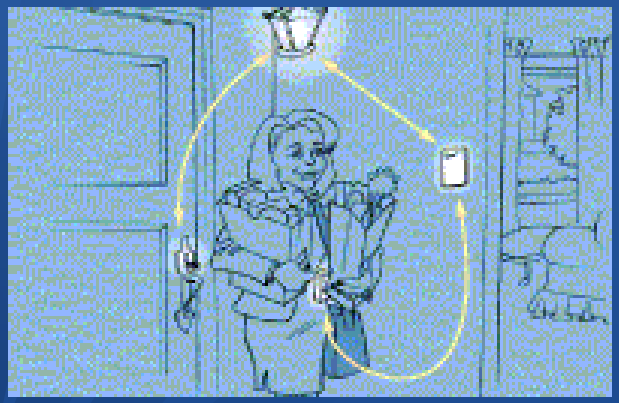


Automatic Synchronization

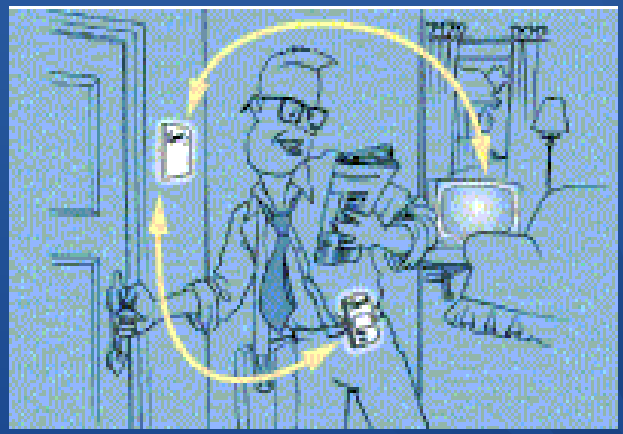


In the Office





At Home



Bluetooth SIG -- more

- February 1998: The Bluetooth SIG 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

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
- 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.

New Application Scenarios

- Data Access Points
- Synchronization
- Headset
- Conference Table
- Cordless Computer
- Business Card Exchange
- Instant Postcard
- Computer Speakerphone

Usage scenarios: Synchronization

User benefits

- **Proximity synchronization**
- **Easily maintained database**
- **Common**

Sharing Common Data…

Usage scenarios: Headset

User benefits

- **Multiple device access**
- **Cordless phone benefits**
- **Hand’s free operation**

Wireless Freedom…

Usage scenarios: Data access points

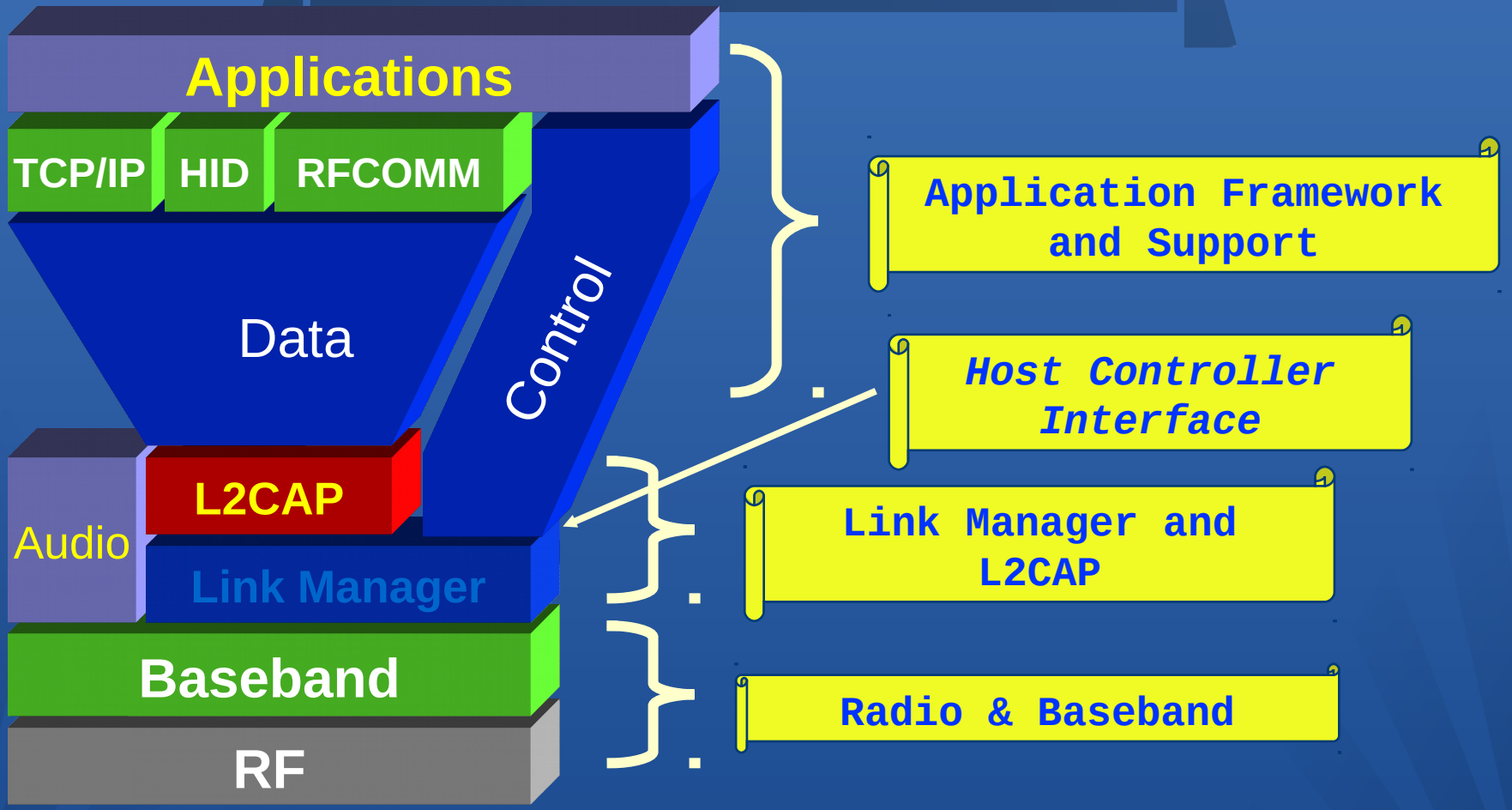
User benefits

- **No more connectors**
- **Easy internet access**
- **Common connection experience**

Remote Connections...

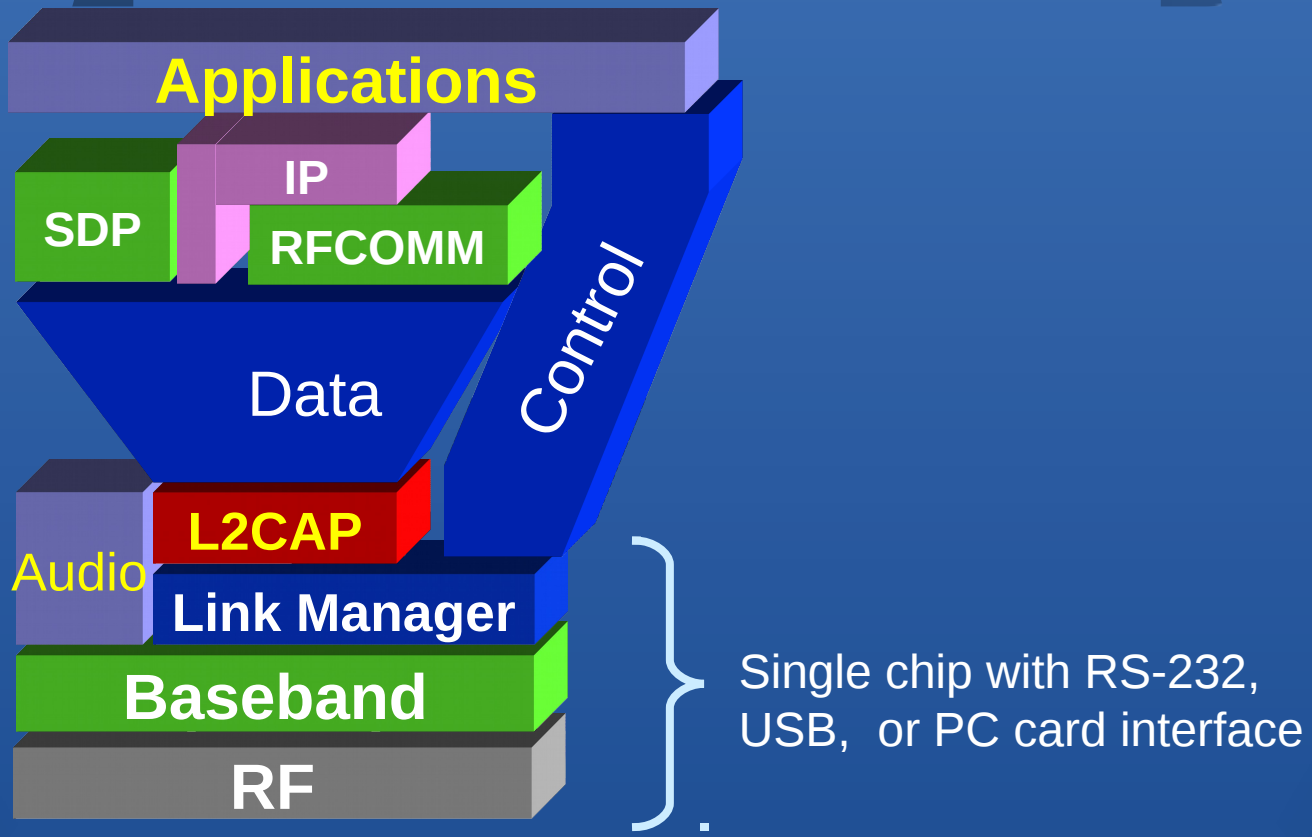
Bluetooth Specifications

What is Bluetooth?



- A hardware/software description
- An application framework

Bluetooth Stack



- A hardware/software/protocol description
- An application framework

Power consciousness

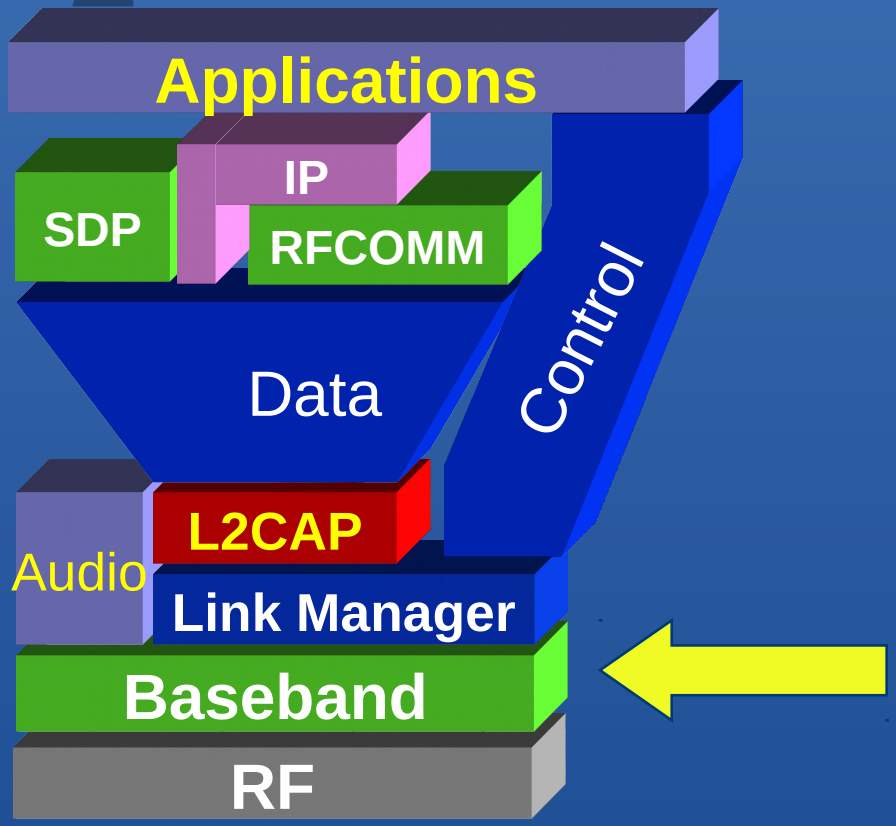
- Standby current < 0.3 mA
  - 3 months(*)
- Voice mode 8-30 mA
  - 75 hours
- Data mode average 5 mA
  (0.3-30mA, 20 kbps, 25%)
  - 120 hours
- Low-power architecture
  - Programmable data length (else radio sleeps)
  - Hold and Park modes: 60 µA
    - Devices connected but not participating
    - Hold retains AMA address, Park releases AMA, gets PMA address
    - Device can participate within 2 ms

(*)**Estimates calculated with 600 mAh battery and internal amplifier, power will vary with implementation**

Radio

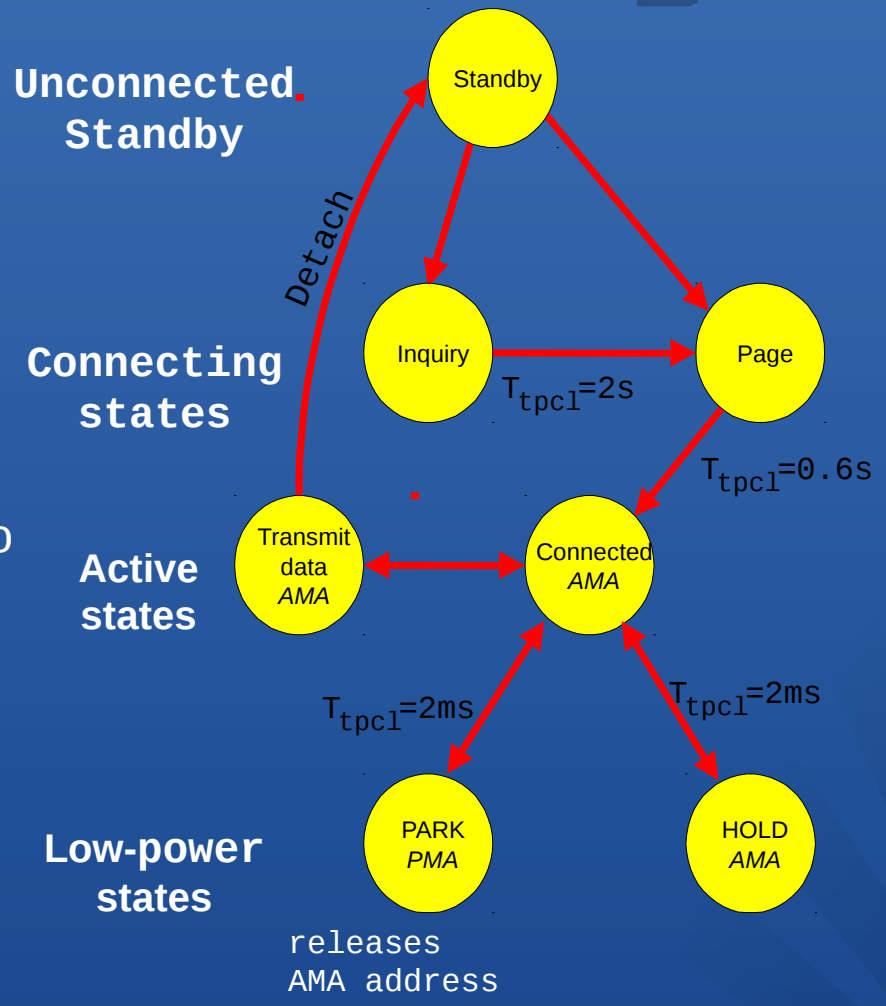
- Low Cost
  - Single chip radio (minimize external components)
  - Today's technology
  - Time division duplex
- Low Power
  - Standby modes
  - Sniff, Hold, Park
  - Low voltage RF
- Robust Operation
  - Fast frequency hopping 1600 hops/sec
  - Strong interference protection
    - Fast ARQ
    - Robust access code
    - Forward header correction

Baseband


Applications
IP
SDP
RFCOMM
Data
Control
L2CAP
Audio
Link Manager
Baseband
RF

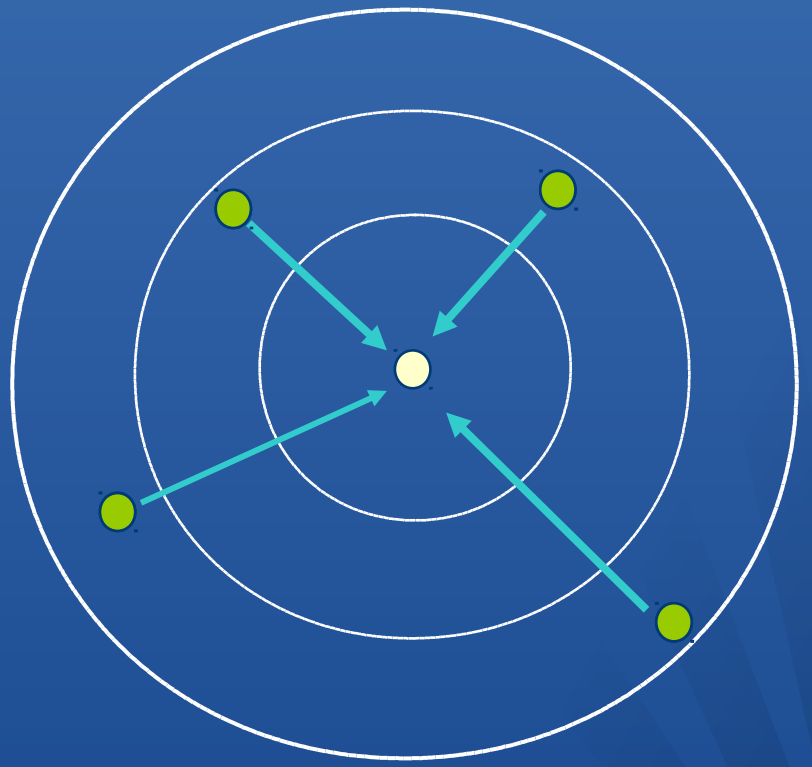
Baseband protocol

- 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/Hold
  - Low-power connected states



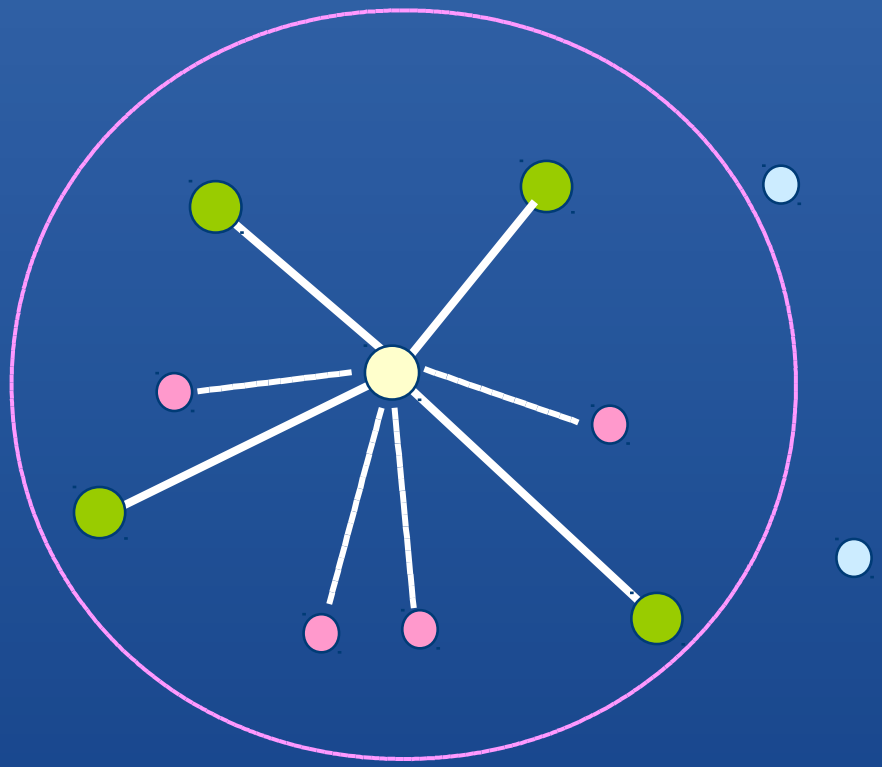
Connection Setup

- Inquiry - scan protocol
  - to lean about the clock offset and device address of other nodes in proximity



Piconet formation

- Page - scan protocol
  - to establish links with nodes in proximity



Master

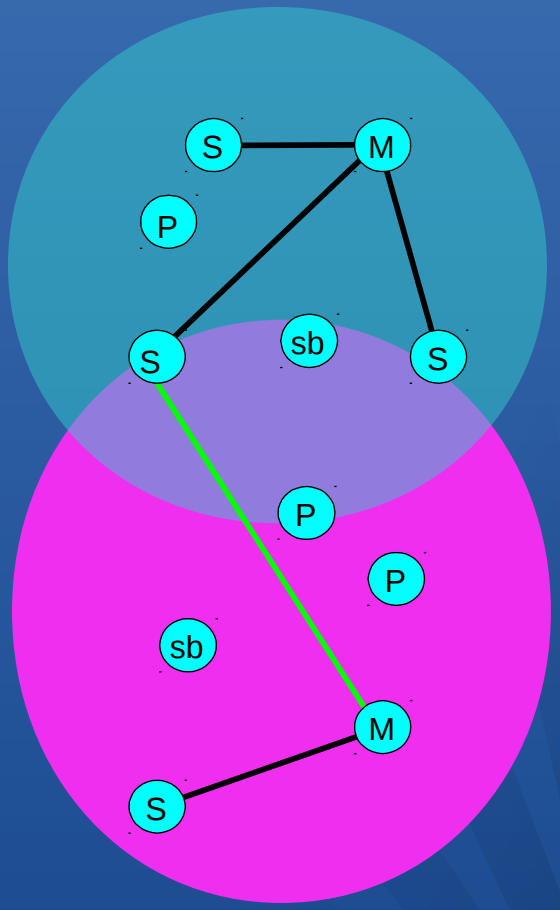
Active Slave

Parked Slave

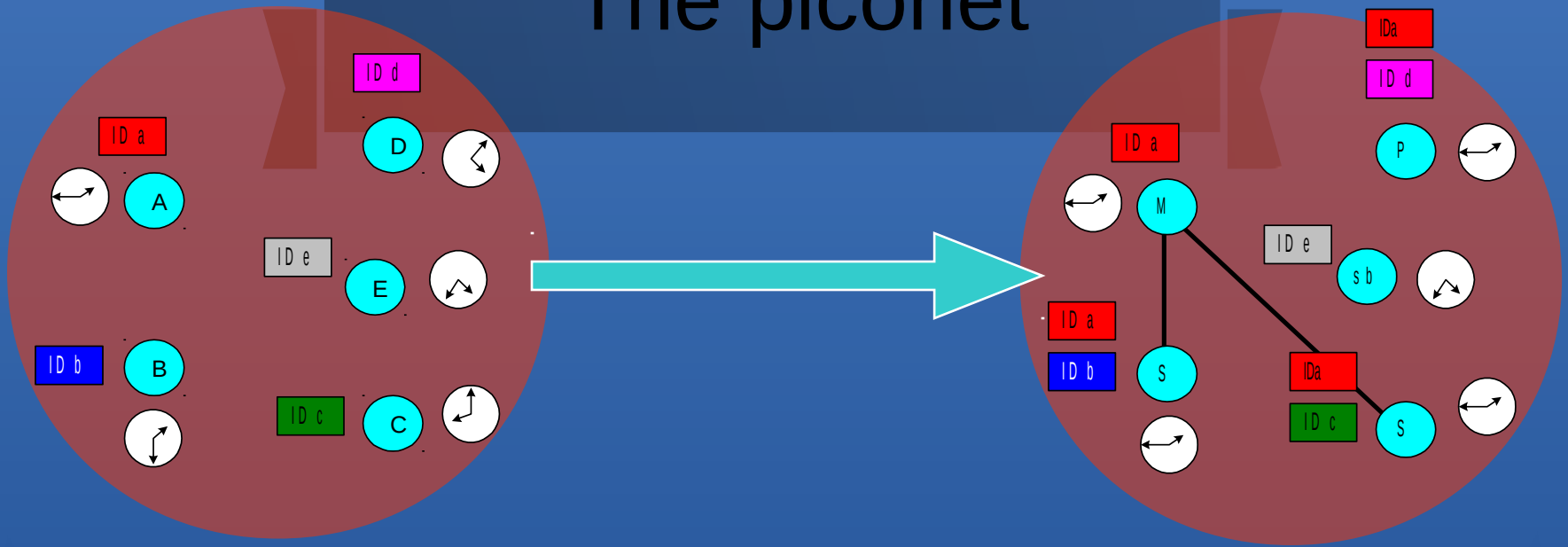
Standby

The Bluetooth network topology

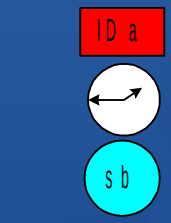
- Radio designation
  - Connected radios can be master or slave
  - Radios are symmetric (same radio can be master or slave)
- Piconet
  - Master can connect to 7 simultaneous or 200+ active slaves per piconet
  - Each piconet has maximum capacity (1 MSps)
  - Unique hopping pattern/ID
- Scatternet
  - High capacity system
  - Minimal impact with up to 10 piconets within range
  - Radios can share piconets!

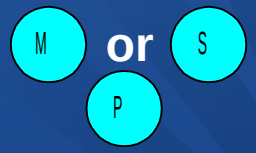


The piconet



- All devices in a piconet hop together
  - To form a piconet: master gives slaves its *clock* and *device ID*
    - Hopping pattern determined by *device ID* (48-bit)
    - Phase in hopping pattern determined by *Clock*
- Non-piconet devices are in standby
- Piconet Addressing
  - Active Member Address (AMA, 3-bits)
  - Parked Member Address (PMA, 8-bits)

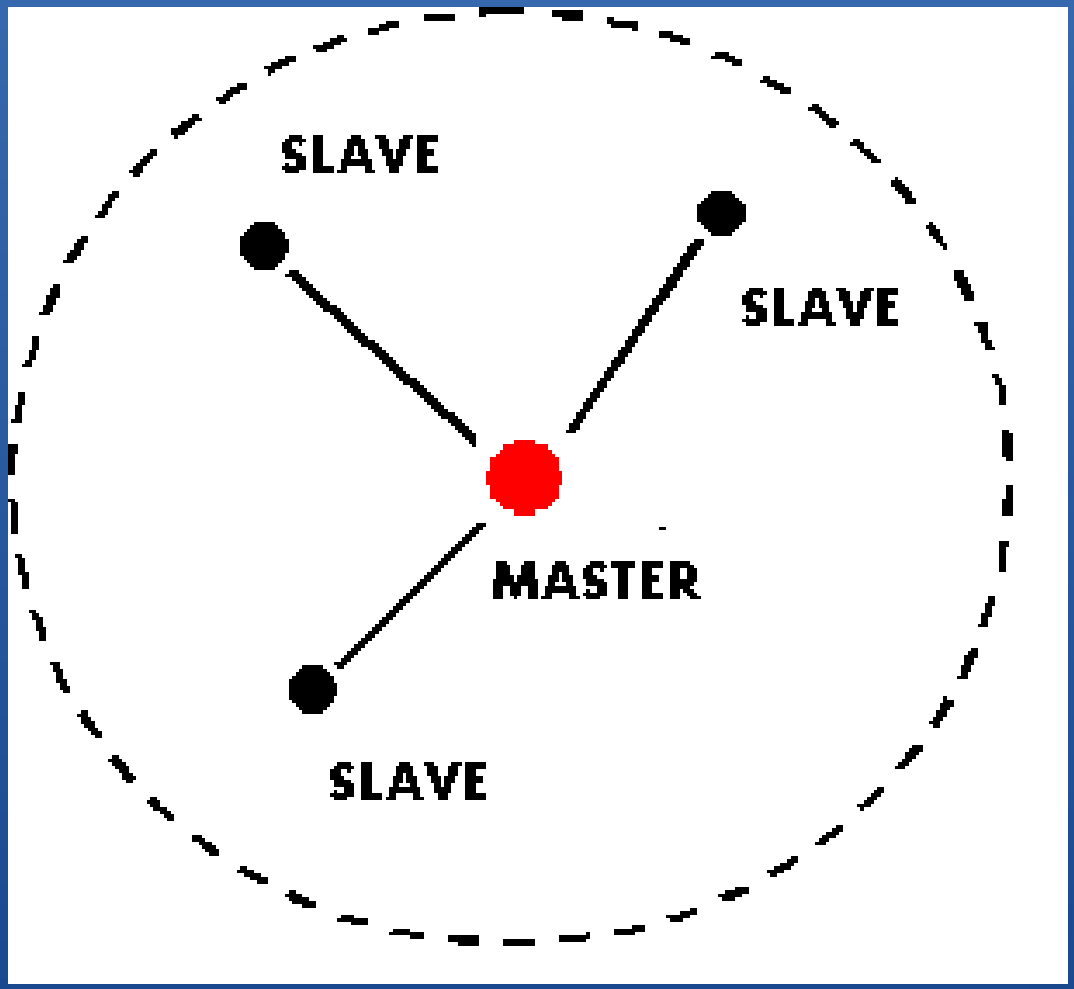




Piconet

- One unit acts as the master of the Piconet, whereas the others acts as slaves.
- Up to seven slaves can be active.
- More slaves can be synchronized & locked to the master in parked state.
- The channel access for all the slaves in a piconet is controlled by the master.

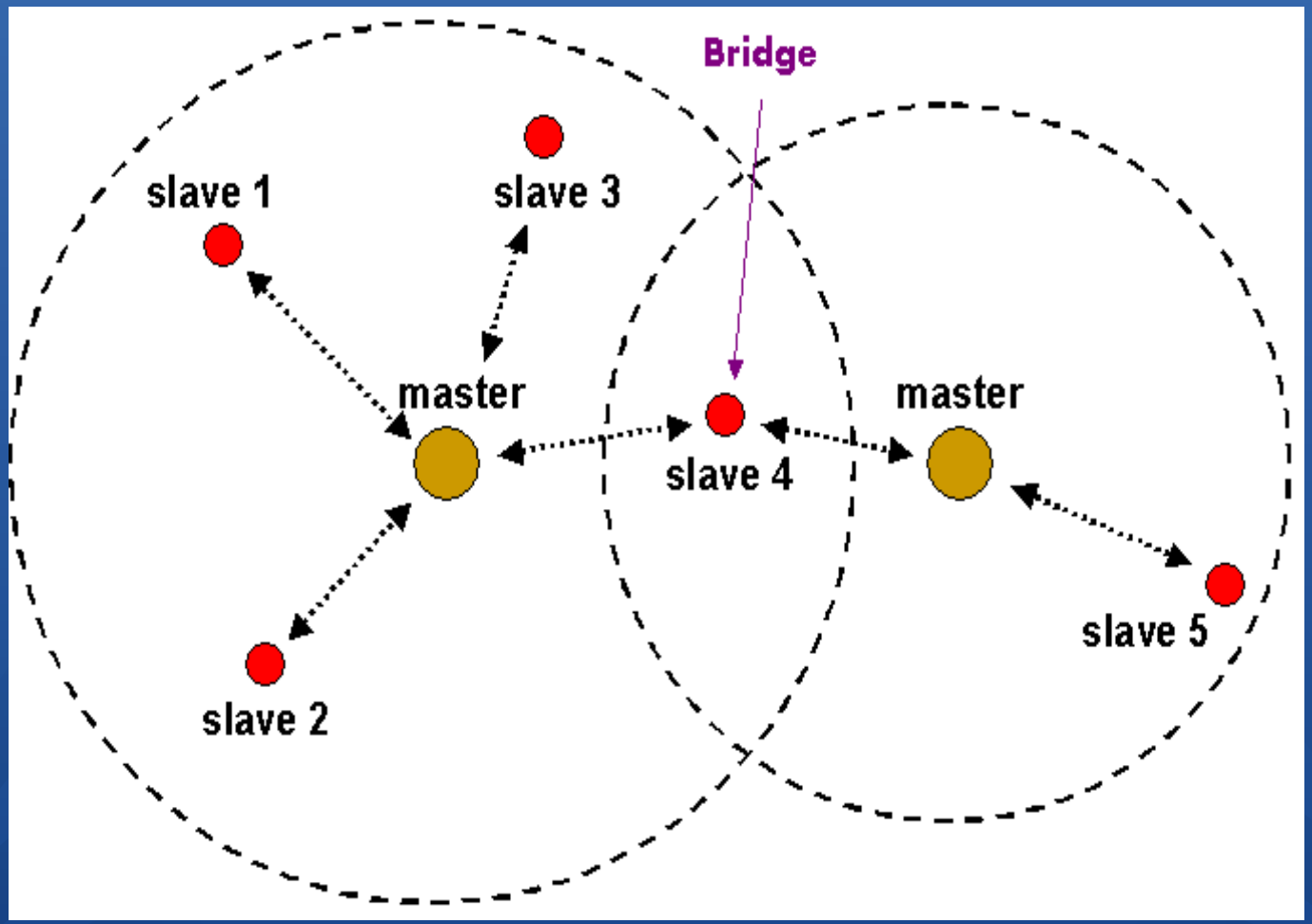
Piconet (2)



Scatternet

- Scatternet is formed by multiple Piconets with overlapping coverage areas.
- Each Piconet can only have a single master
- Slaves can participate in different Piconets on a time-division multiplex basis.
- A master in one Piconet can be a slave in another Piconet.
- Each Piconet has its own hopping channel in a Scatternet.

Scatternet (2)

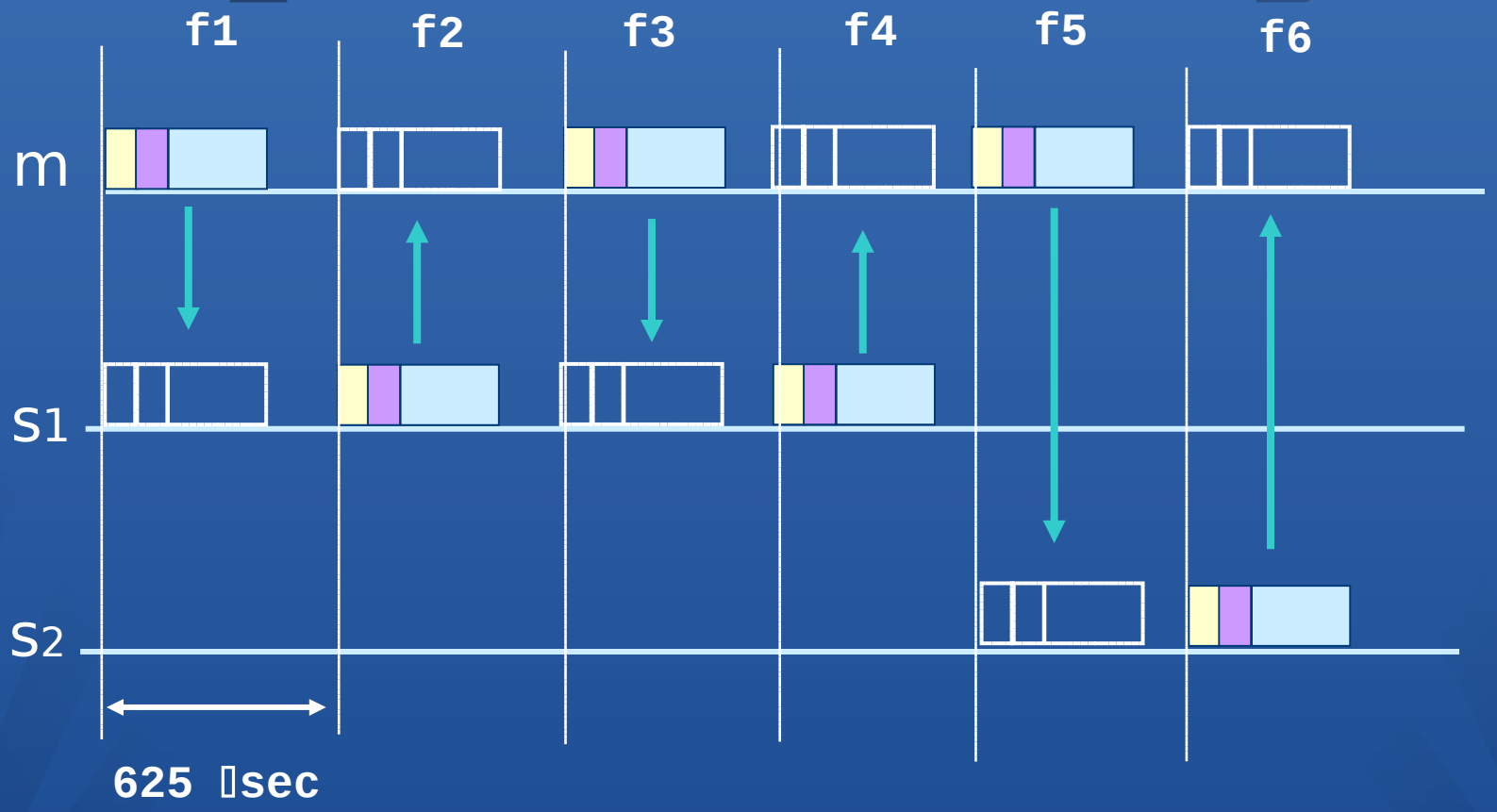


Addressing

- 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

Piconet channel

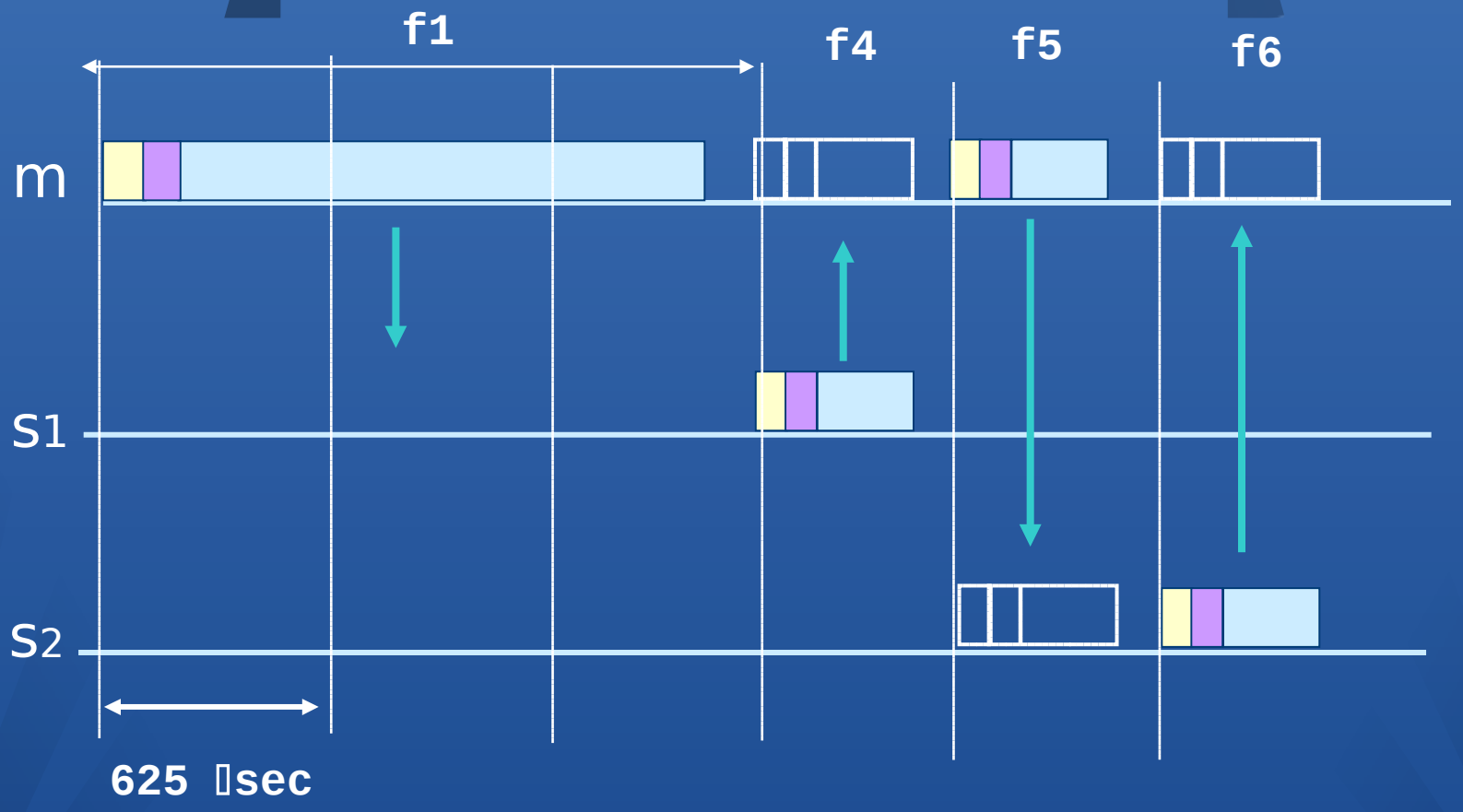
FH/TDD



1600 hops/sec

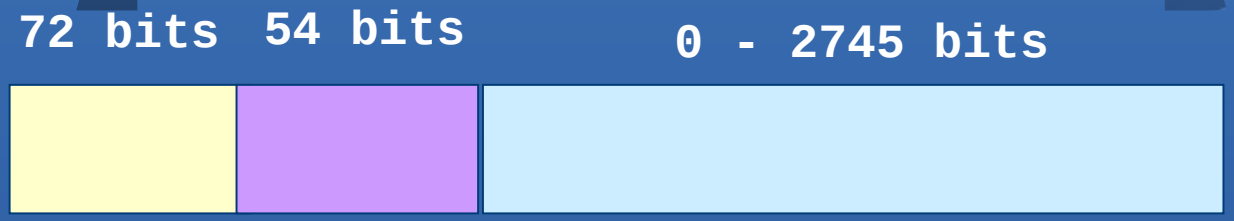
Multi slot packets

FH/TDD



Data rate depends on type of packet

Packet Format



Access code

Synchronization
identification
Filtering

Header

Address
Packet Type
Flow control
ARQ
SEQN
HEC

Payload

Error correction
1/3 rate FEC
2/3 rate FEC
ARQ scheme for the data

Smaller than an ATM cell !
Notice that there is no protocol type field

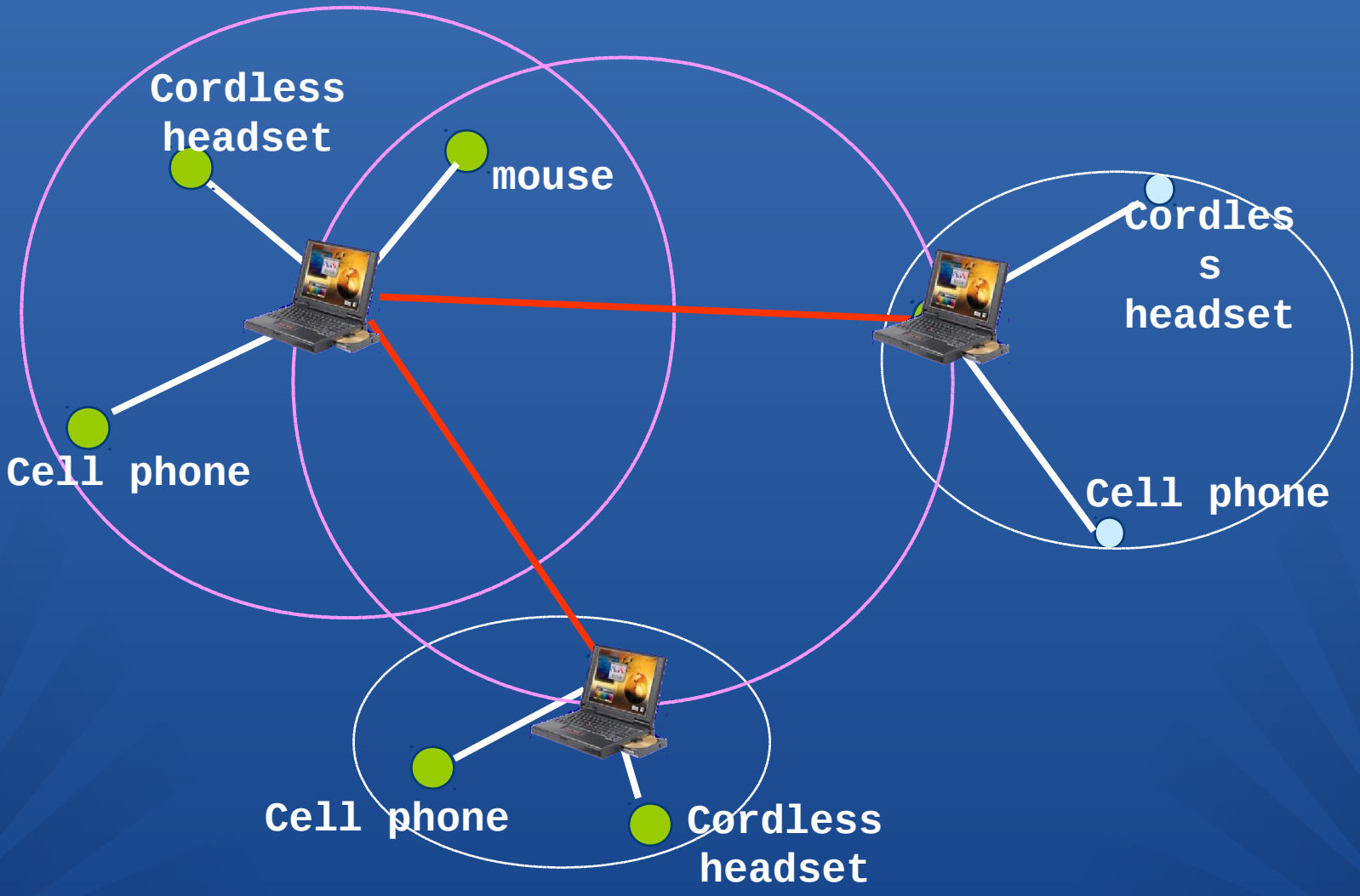
Physical Link Types

- Synchronous Connection Oriented (SCO) Link
  - slot reservation at fixed intervals
    - No ARQ, No CRC
    - FEC (optional)
    - 64 Kbps
- Asynchronous Connection-less (ACL) Link
  - Polling access method
  - ARQ, CRC
  - FEC (optional)
  - Symmetric data rate 108 - 433 Kbps
  - Asymmetric data rate up to 723 Kbps

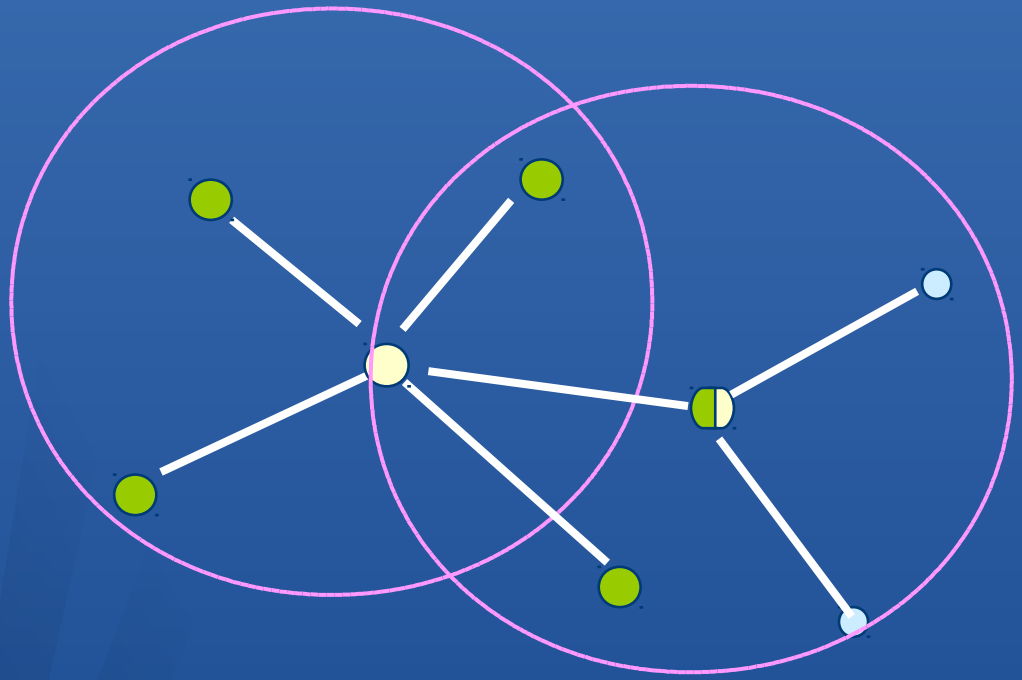
Error handling

- Forward-error correction (FEC)
  - headers are protected with 1/3 rate FEC and HEC
  - payloads may be FEC protected
    - 1/3 rate: simple bit repetition (SCO packets only)
    - 2/3 rate: (10,15) shortened Hamming code
    - 3/3 rate: no FEC
- ARQ (ACL packets only)
  - 16-bit CRC (CRC-CCITT) & 1-bit ACK/NACK
  - 1-bit sequence number

Inter piconet communication



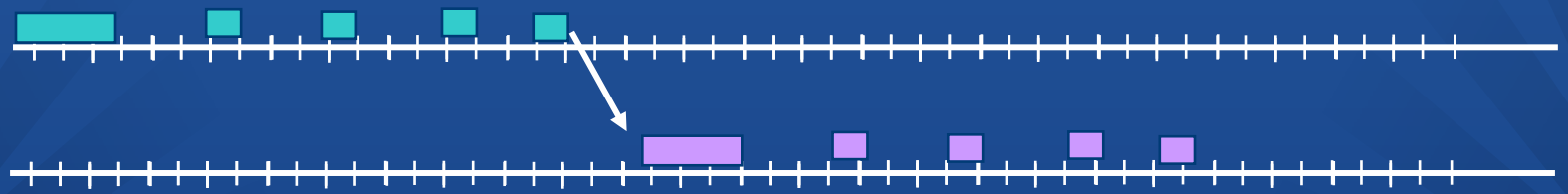
Scatternet, scenario



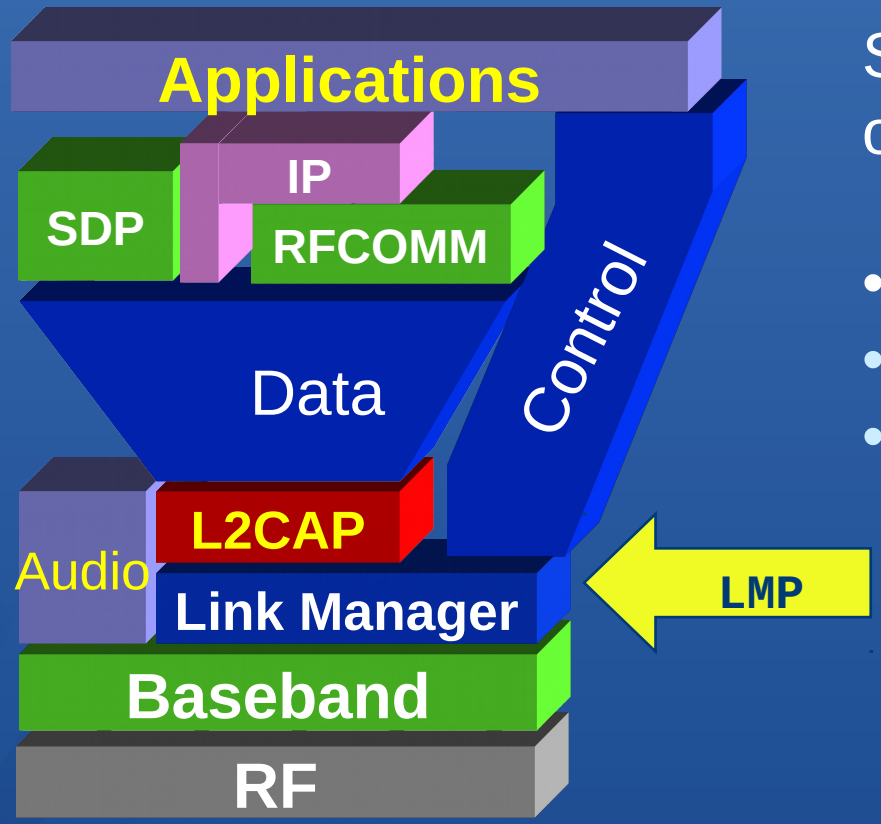
How to schedule presence in two piconets?

Forwarding delay ?

Missed traffic?



Link Manager Protocol



Setup and Management of Baseband connections

- Piconet Management
- Link Configuration
- Security

Link Manager Protocol

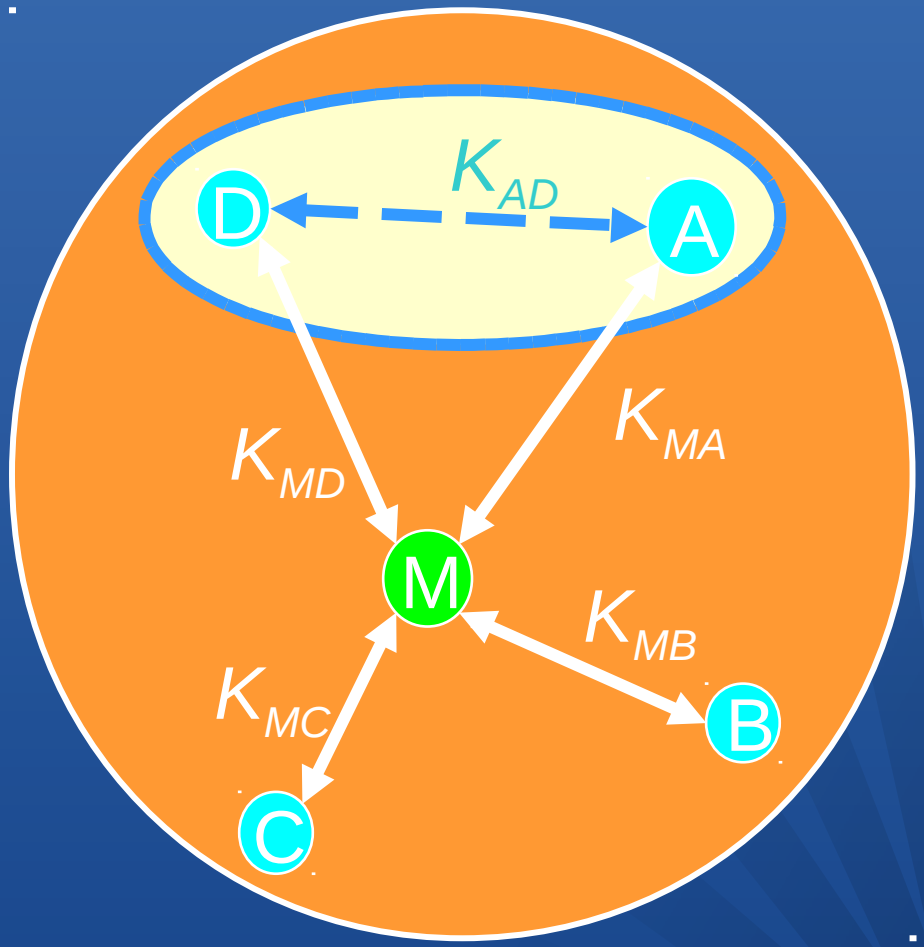
- Piconet Management
  - Attach and detach slaves
  - Master-slave switch
  - Establishing SCO and ACL links
  - Handling of low power modes (Sniff, Hold, Park)
- Link Configuration
  - packet type negotiation
  - power control
- Security functions
  - Authentication
  - Encryption

Bluetooth security features

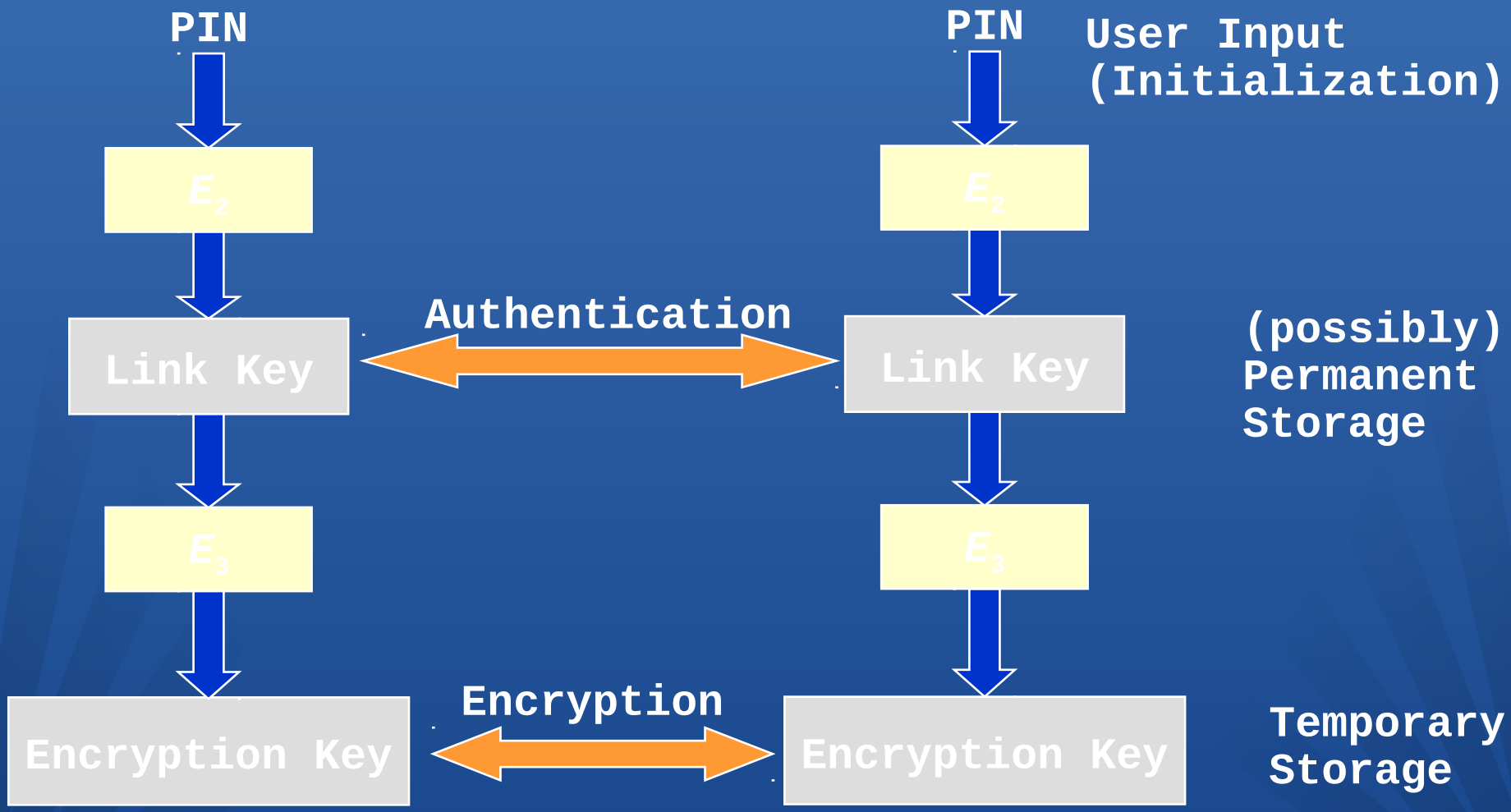
- Fast frequency hopping (79 channels)
- Low transmit power (range <= 10m)
- Authentication of remote device
  - based on link key (128 Bit)
  - May be performed in both directions
- Encryption of payload data
  - Stream cipher algorithm (≤ 128 Bit)
  - Affects all traffic on a link
- Initialization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



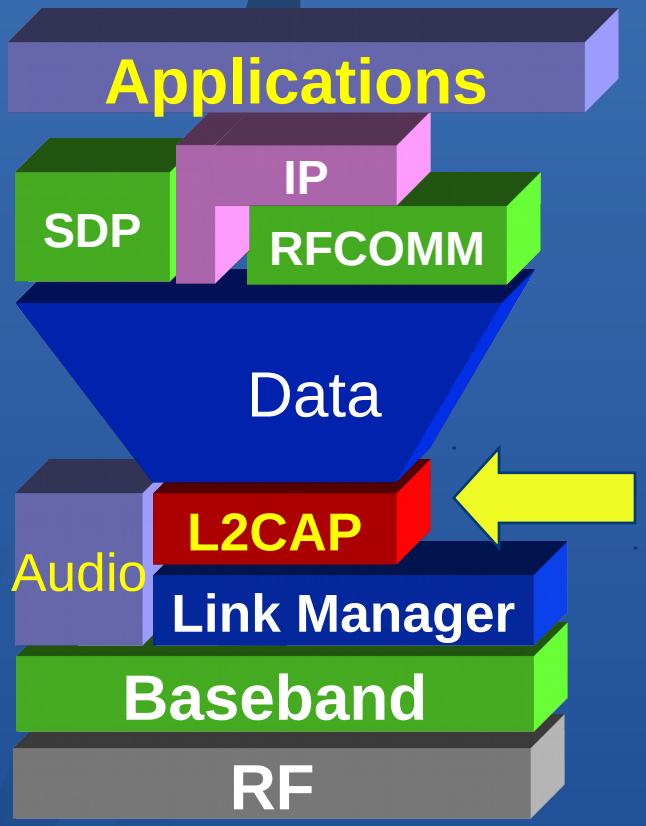
Key generation and usage



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

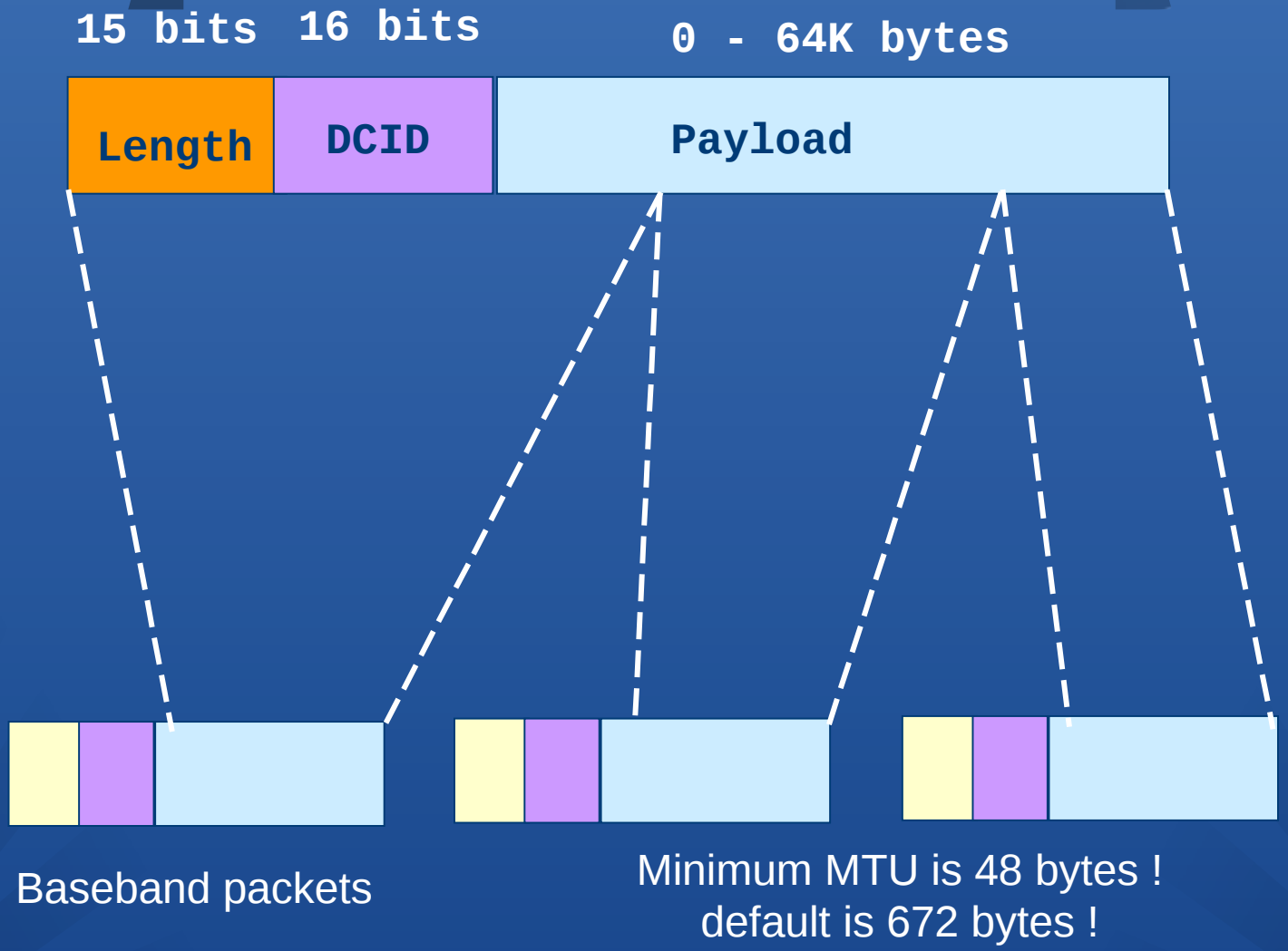
L2CAP



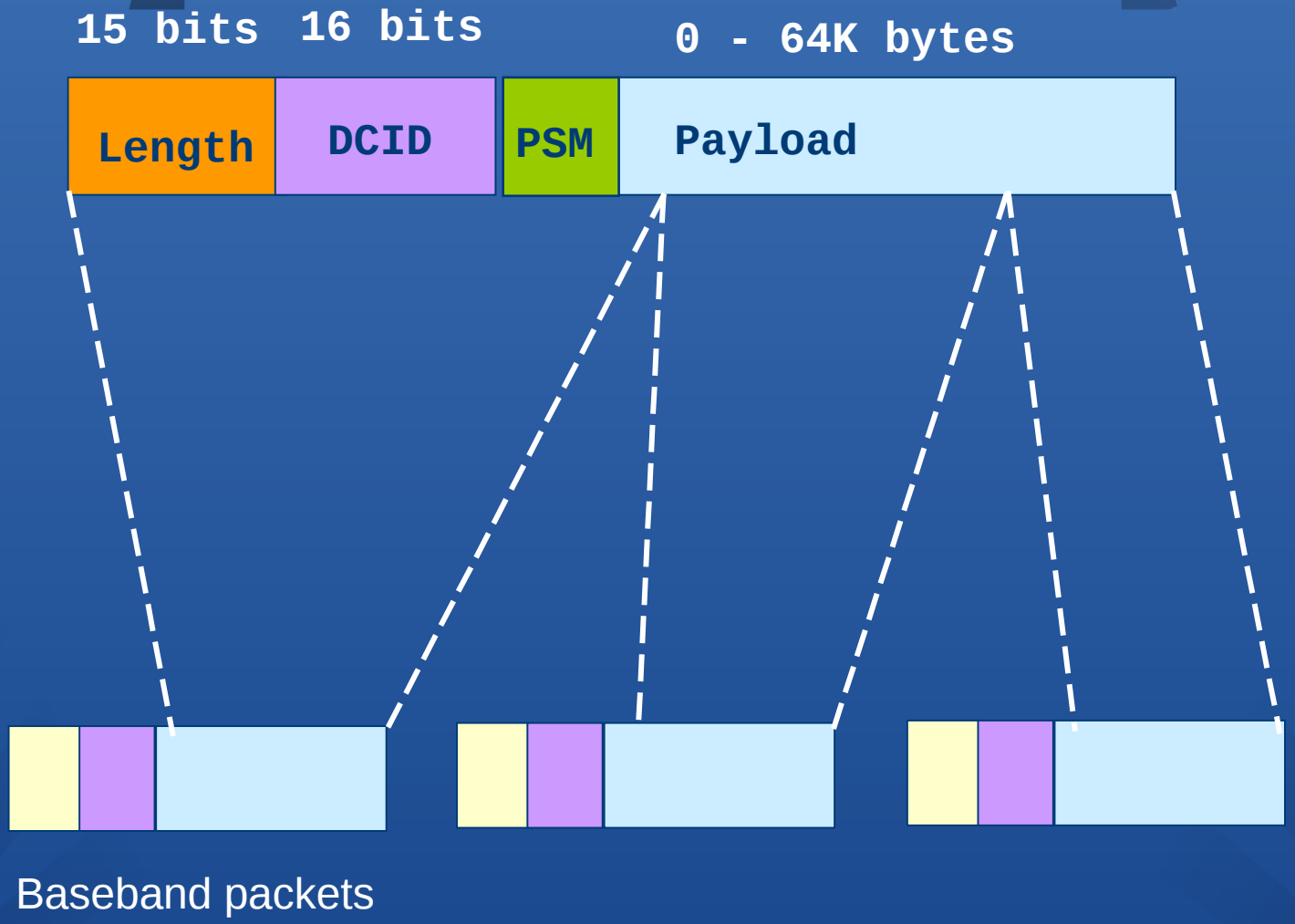
Logical Link Control and Adaptation Protocol

- L2CAP provides
  - Protocol multiplexing
  - Segmentation and Re-assembly
  - Quality of service negotiation
  - Group abstraction

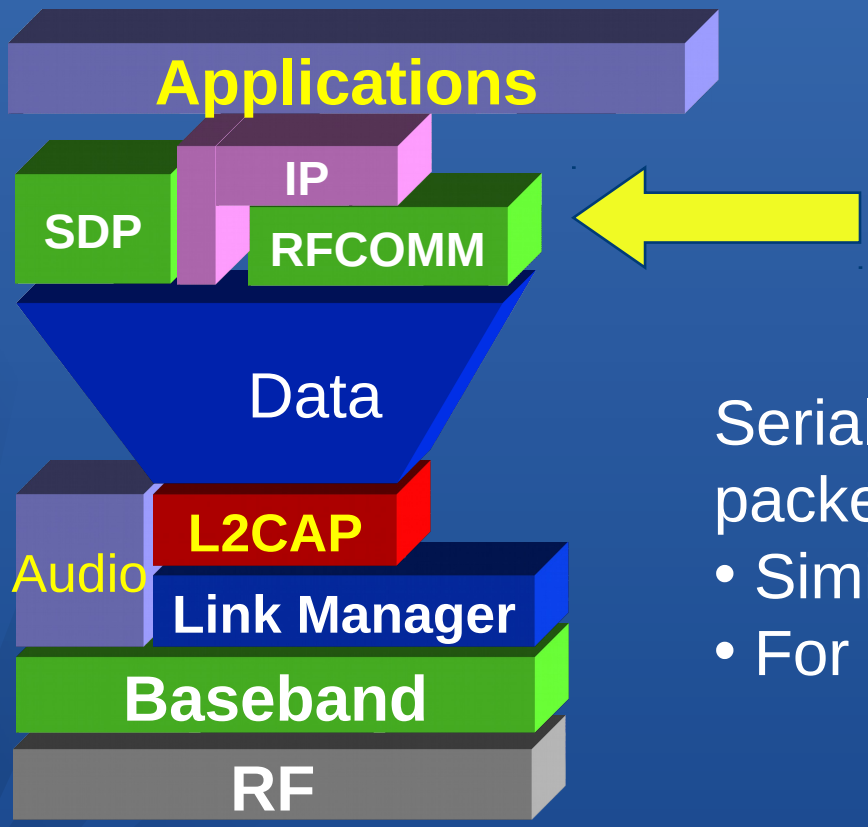
L2CAP Packet Format (CO)



L2CAP Packet Format (CL)



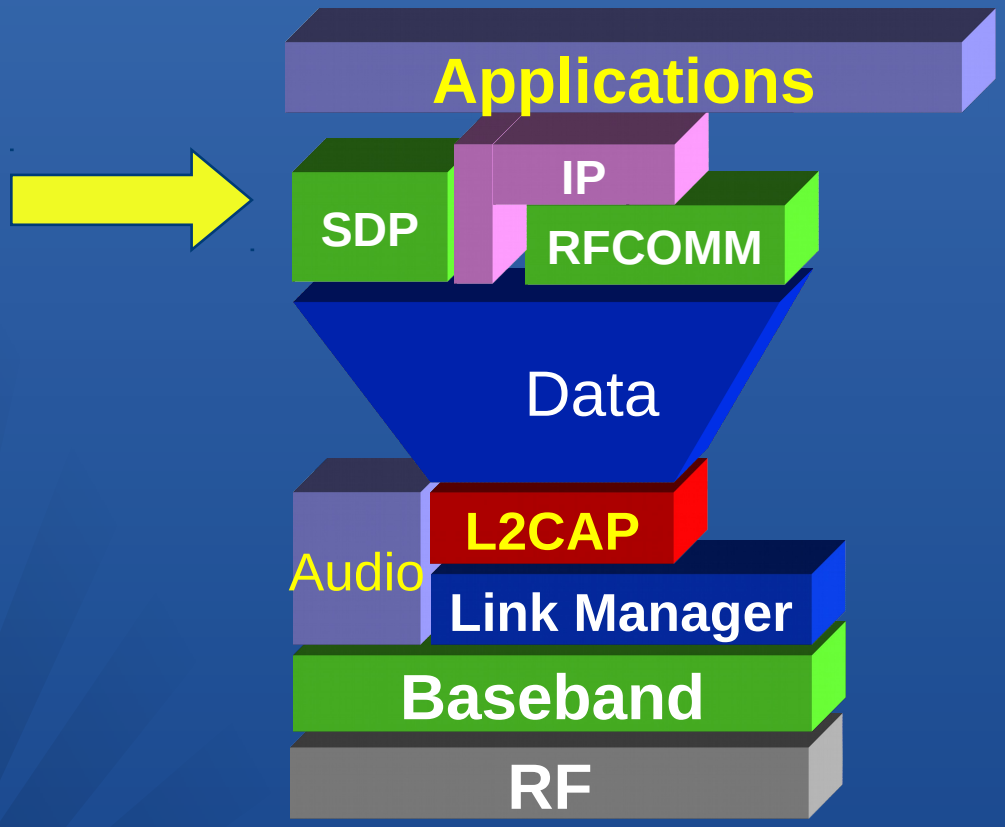
Serial Port Emulation using RFCOMM



Serial Port emulation on top of a packet oriented link

- Similar to HDLC
- For supporting legacy apps

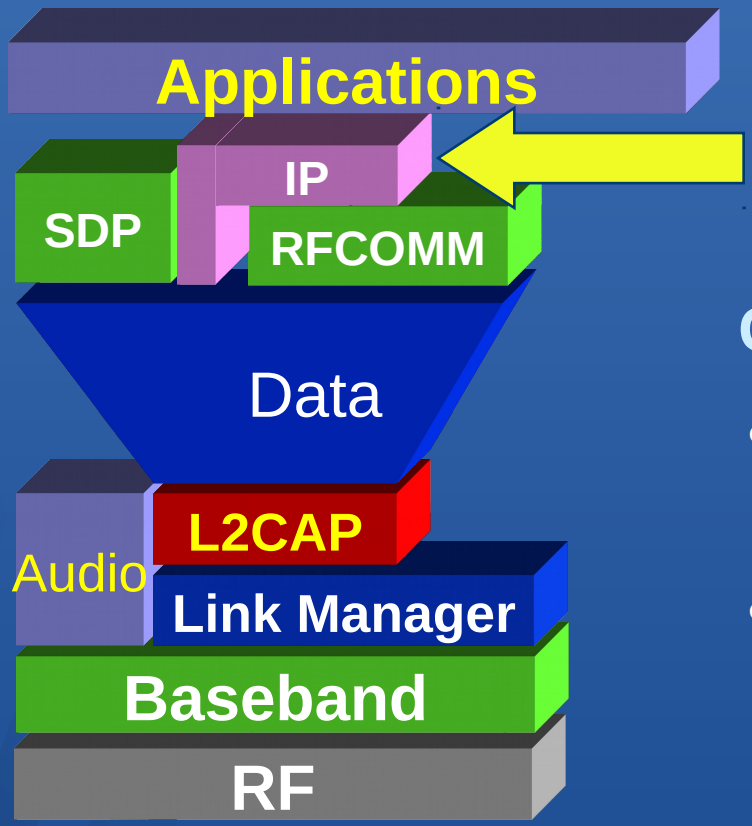
Bluetooth Service Discovery Protocol



Usage of SDP

- Establish L2CAP connection to remote device
- Query for services
  - search for specific class of service, or
  - browse for services
- Retrieve attributes that detail how to connect to the service
- Establish a separate (non-SDP) connection to user the service

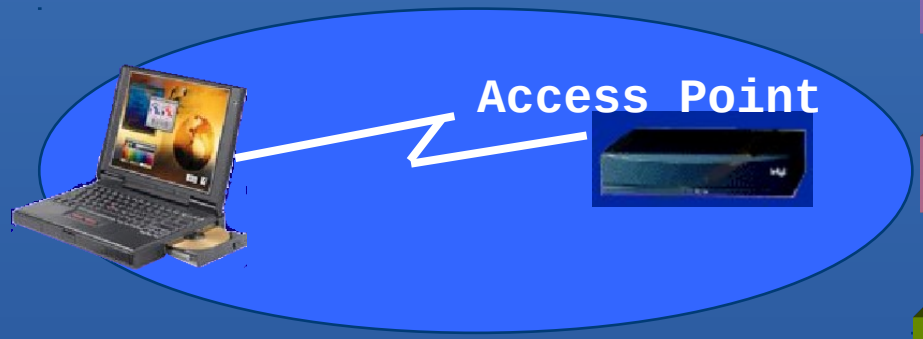
IP over Bluetooth V 1.0



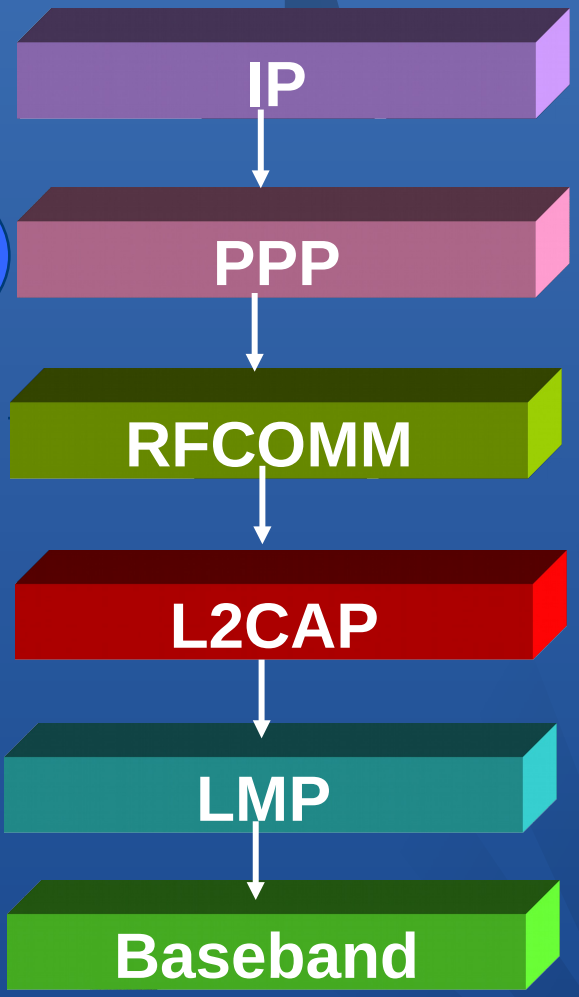
GOALS

- Internet access using cell phones
- Connect PDA devices & laptop computers to the Internet via LAN access points

LAN access point profile



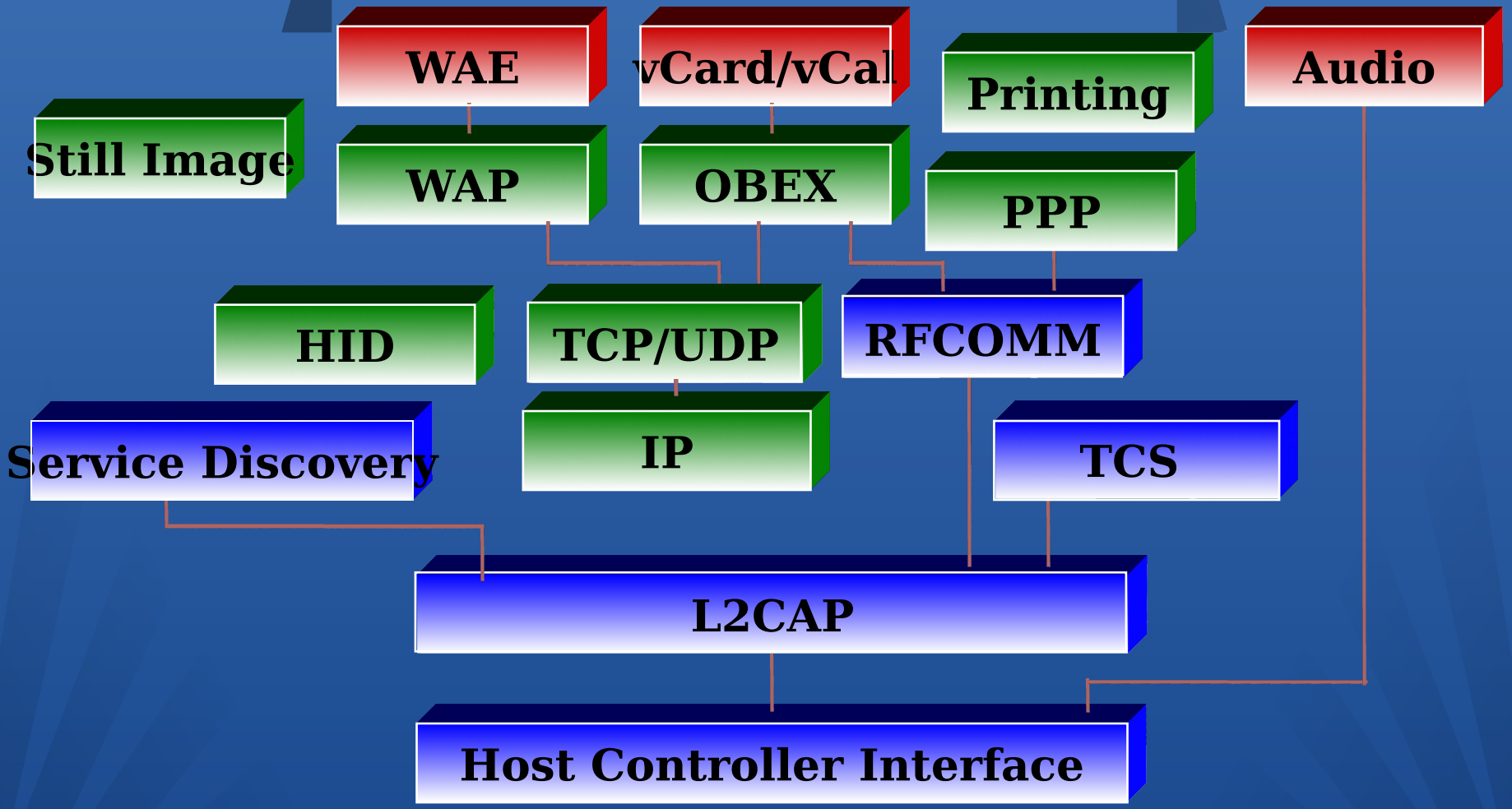
- Security
  - Authentication
  - Access control
- Efficiency
  - header and data compression
- Auto-configuration
- Lower barrier for deployment



Software architecture goals

- Support the target usage scenarios
- Support a variety of hardware platforms
- Good out of box user experience
  - Enable legacy applications
  - Utilize existing protocols where possible

Bluetooth protocols



Bluetooth protocols

- Host Controller Interface (HCI)
  - provides a common interface between the Bluetooth host and a Bluetooth module
    - Interfaces in spec 1.0: USB; UART; RS-232
- Link Layer Control & Adaptation (L2CAP)
  - A simple data link protocol on top of the baseband
    - connection-oriented & connectionless
    - protocol multiplexing
    - segmentation & reassembly
    - QoS flow specification per connection (channel)
    - group abstraction

Bluetooth protocols

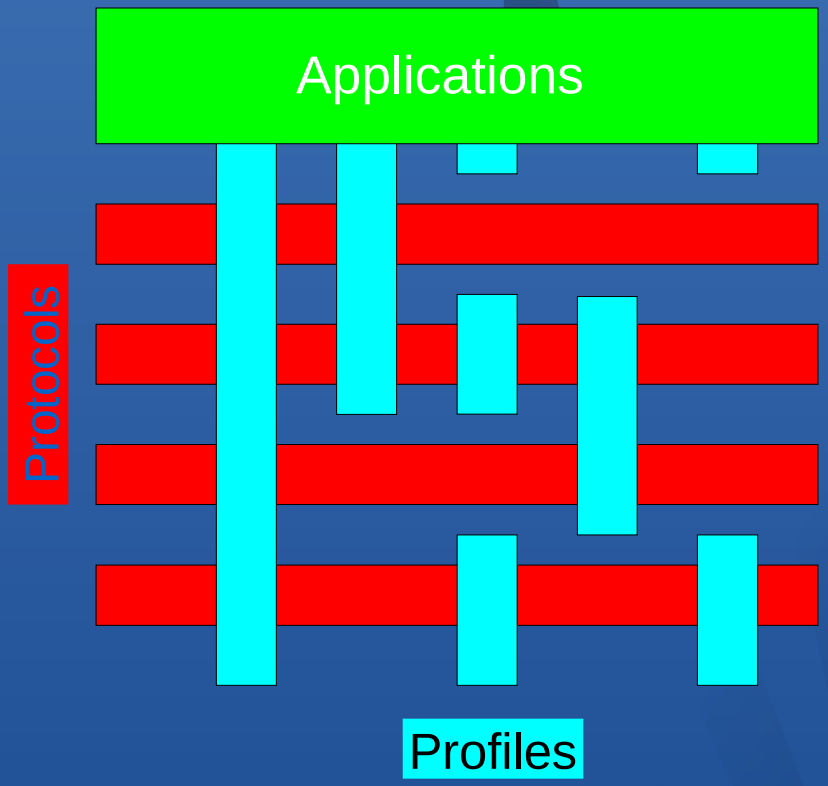
- Service Discovery Protocol (SDP)
  - Defines a service record format
    - Information about services provided by *attributes*
    - Attributes composed of an ID (name) and a value
    - IDs may be universally unique identifiers (UUIDs)
  - Defines an inquiry/response protocol for discovering services
    - Searching for and browsing services

Bluetooth protocols

- RFCOMM (based on GSM TS07.10)
  - emulates a serial-port to support a large base of legacy (serial-port-based) applications
  - allows multiple “ports” over a single physical channel between two devices
- Telephony Control Protocol Spec (TCS)
  - call control (setup & release)
  - group management for gateway serving multiple devices
- Legacy protocol reuse
  - resuse existing protocols, e.g., IrDA’s OBEX, or WAP for interacting with applications on phones

Interoperability & Profiles

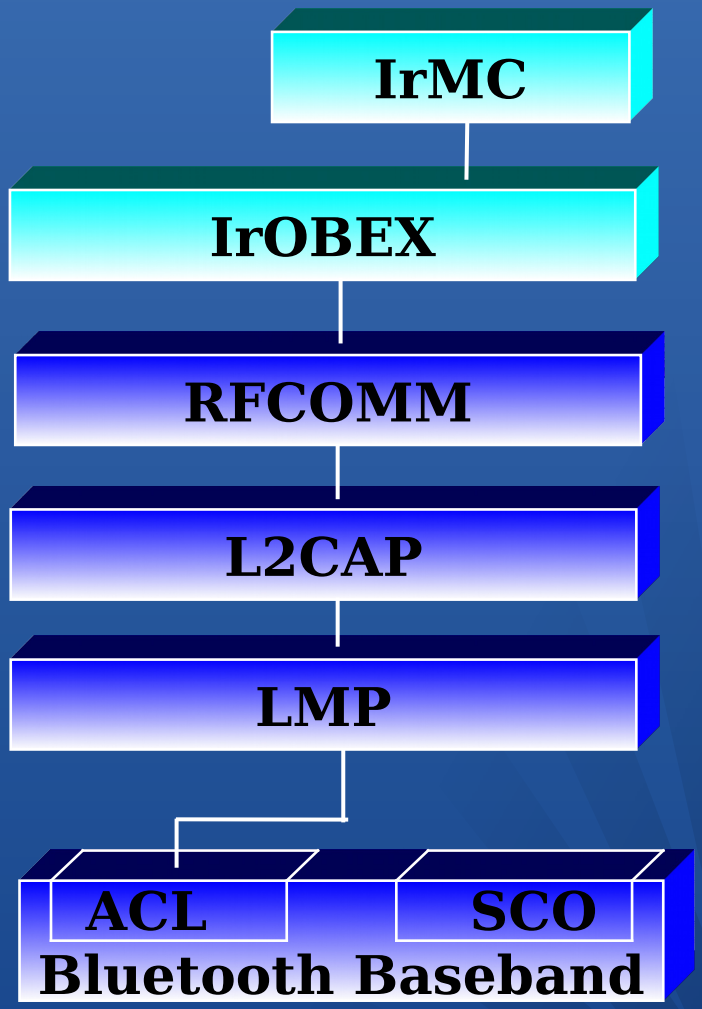
- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles



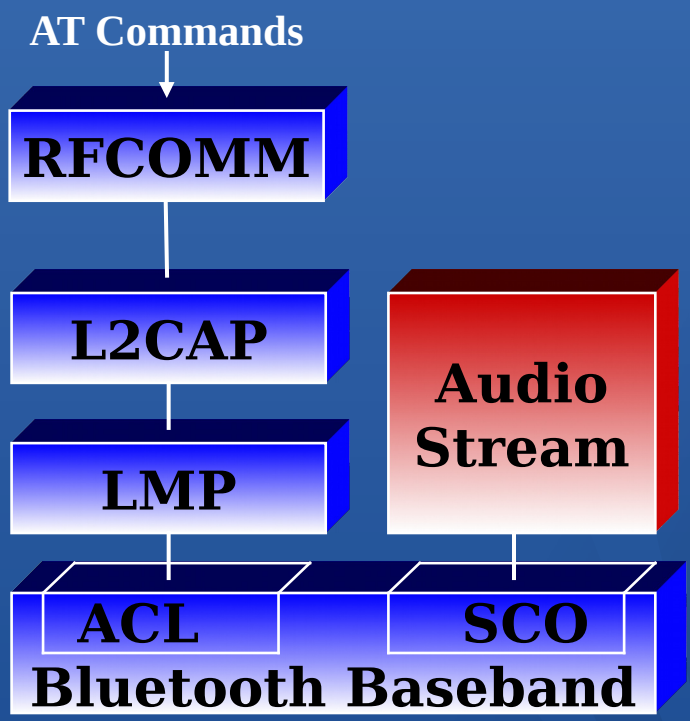
Profiles

- Generic Access Profile
  - Service Discovery Application Profile
  - Serial Port Profile
    - Dial-up Networking Profile
    - Fax Profile
    - Headset Profile
    - LAN Access Profile (using PPP)
    - Generic Object Exchange Profile
      - File Transfer Profile
      - Object Push Profile
      - Synchronization Profile
  - *TCS_BIN-based profiles*
    - Cordless Telephony Profile
    - Intercom Profile

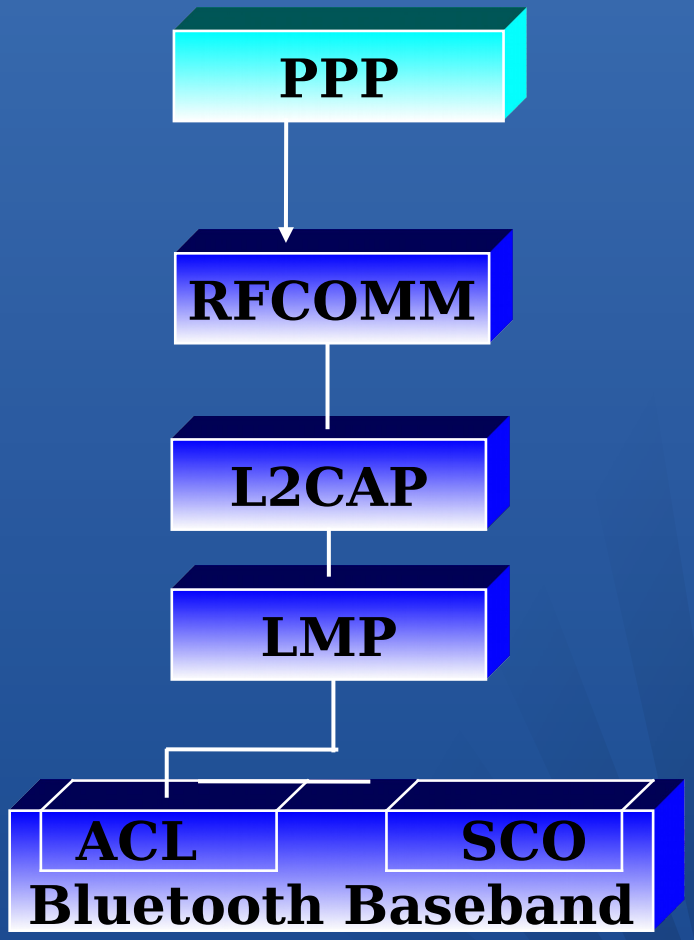
Synchronization profile



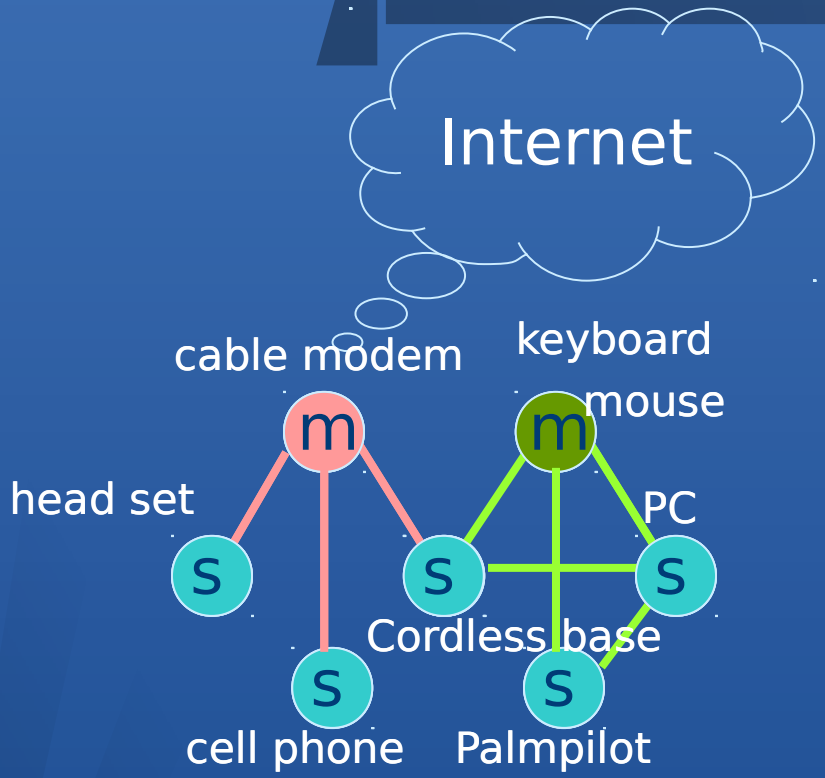
Headset profile



LAN access point profile



Research challenges



Plug-n-play applications

Resource Discovery

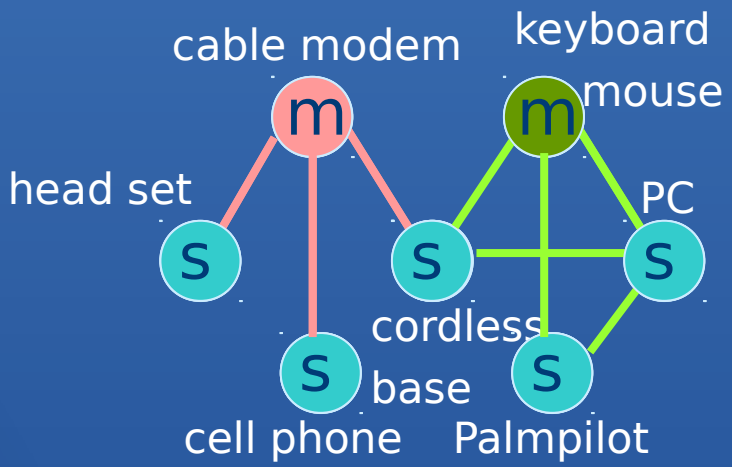
Routing over scatternets

Techniques for link formation

Techniques for Scatternets Formation

Will the current solutions for each layer work in this environment?

What is different in this scenario ?



Connection oriented, low-power link technology

Small, multi-hop networks

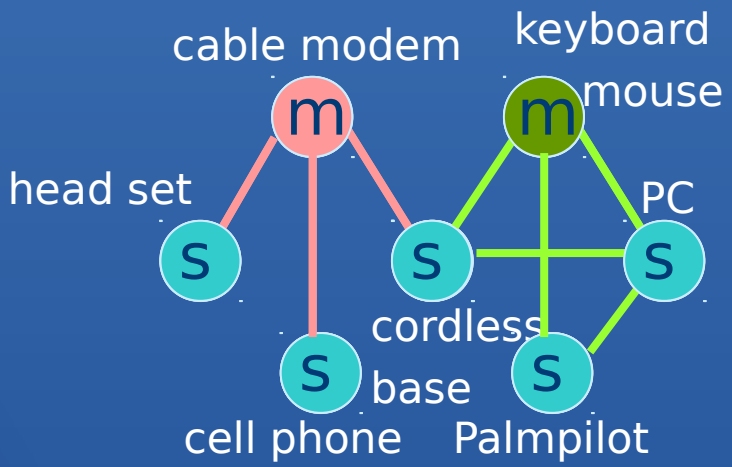
Simple devices

Isolated network

Dynamic network

Applications ---> services ----> routing ----> link creation

Service discovery

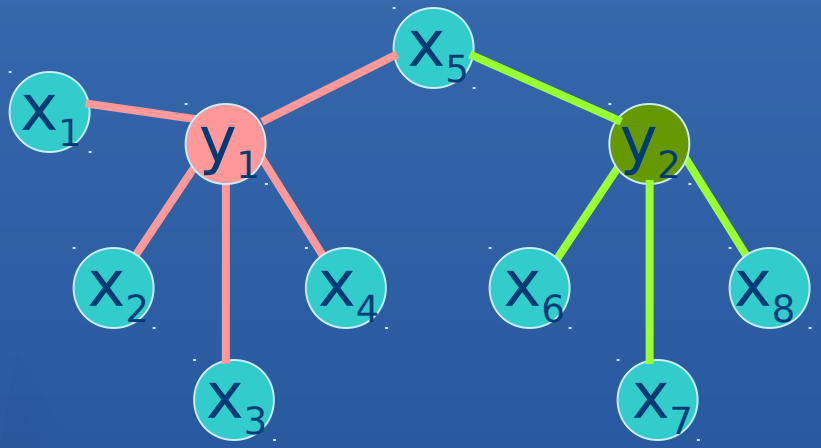


Need solutions for address allocation, name resolution, service discovery

Existing solutions in the Internet depend on infrastructure

Judicious use of Multicast/broadcast is needed

Routing over Scatternets



Nodes must co-operate to forward packets (MANET style protocols)

Forwarding at Layer 2 or Layer 3?

Bridging or routing ?

What interface should be exported to the above layer?

Better coupling with the service discovery layer is needed

Summary

- Bluetooth is a global, RF-based (ISM band: 2.4GHz), short-range, connectivity technology & solution for portable, personal devices
  - it is not just a radio
  - create piconets on-the-fly (appr. 1Mbps)
    - piconets may overlap in time and space for high aggregate bandwidth
- The Bluetooth spec comprises
  - a HW & SW protocol specification
  - usage case scenario profiles and interoperability requirements
- 1999 Discover Magazine Awards finalist
- To learn more: *http://www.bluetooth.com*