Bluetooth™

Dominique Chomienne & Michel Eftimakis

NewLogic

Tutorial Agenda

- **Bluetooth Marketing view**
- **Bluetooth network topology**
- **Bluetooth protocol**
  - RF
  - Baseband
  - LC, LM
  - HCI
  - L2CAP
  - Higher layers
- **Bluetooth implementation**
- **Bluetooth “live” demo !!!**

Bluetooth™

Tutorial

NewLogic

Bluetooth™ Marketing View

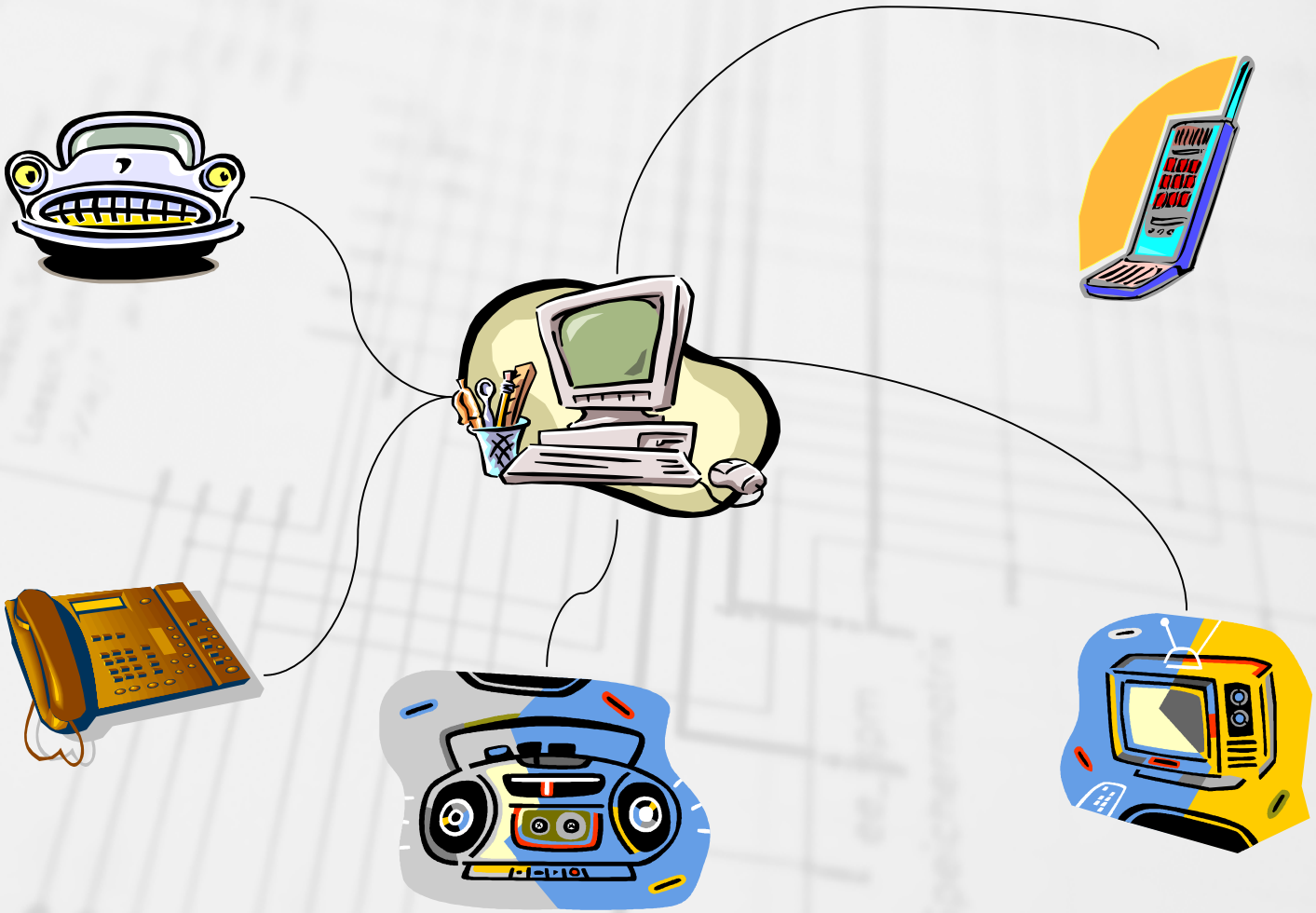
Marketing slides ahead

Bluetooth™

Tutorial

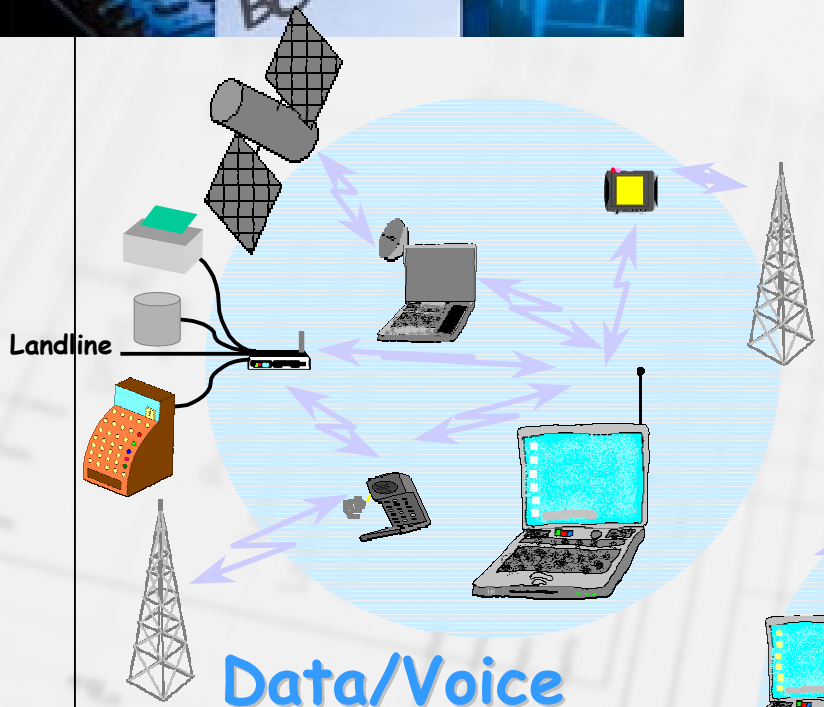
NewLogic

Bluetooth™ The Last Ten Meters



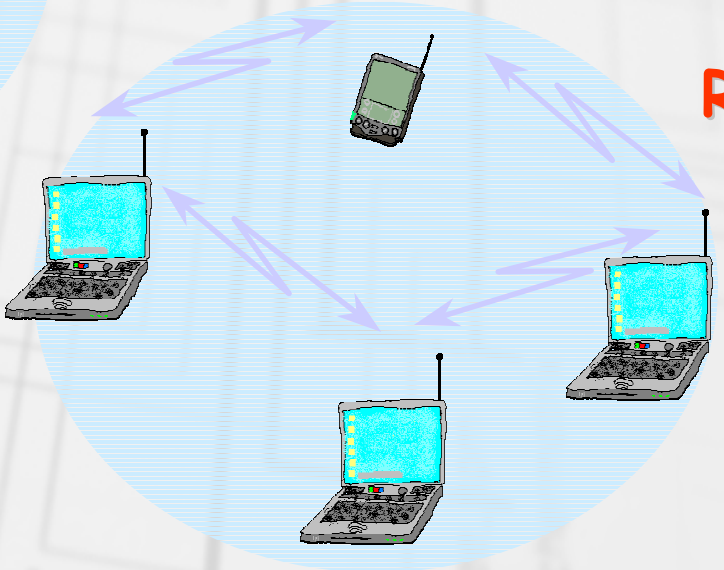
NewLogic

Bluetooth™ Systems



Data/Voice Access Points

Cable Replacement



Personal Ad-hoc Networks

Bluetooth™

NewLogic

Bluetooth™ Target products

Intelligent Devices

- PCs
- Cellular Phones
- PDAs

Audio Peripherals

- Headsets
- Speakers
- Stereo Receiver

Data Peripherals

- Mice
- Keyboards
- Joysticks
- Cameras
- Digital Pens
- Printers
- LAN access points

Embedded Applications

- Cars: Power lock controls
- Grocery store updates
- Closed Systems
- Industrial systems
- MIDI musical instruments

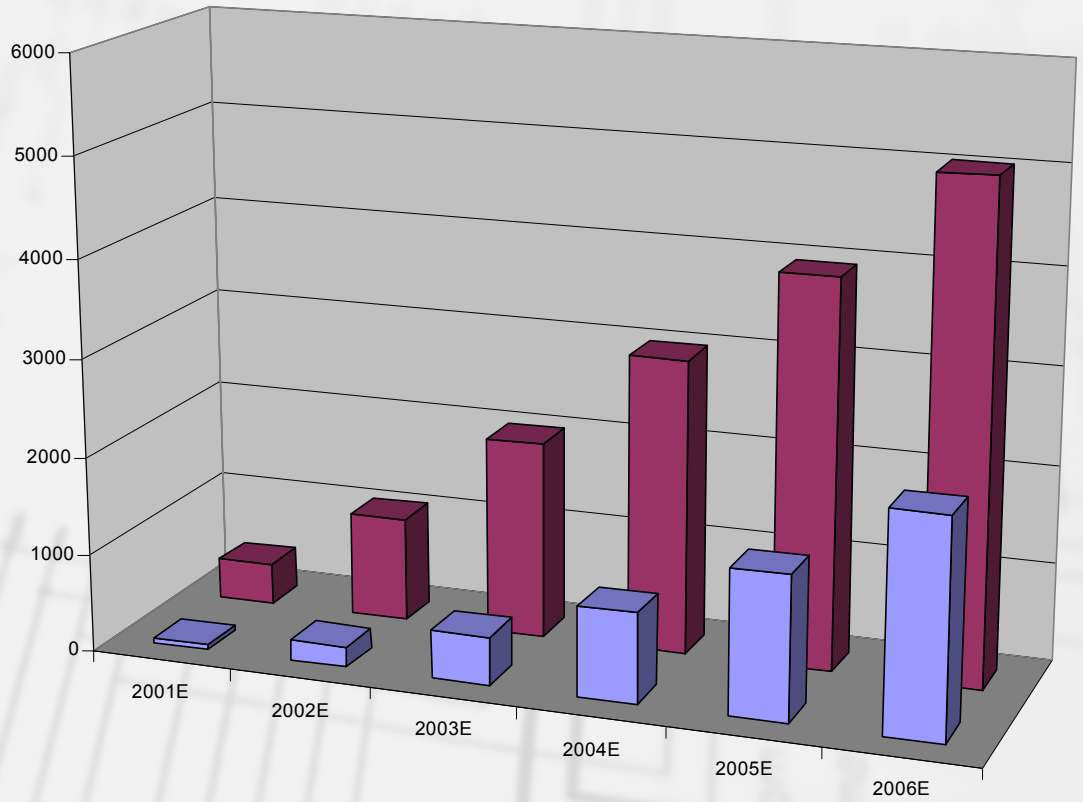
Bluetooth™ Usage Models

- Computer to Computer File Transfer
- Dialup Networking
- Synchronization
- 3 in 1 Phone
- Ultimate Headset
- Computer Speakerphone
- Cordless Computer
- Instant Postcard
- Hidden Computing
- Conference Table
- …

Bluetooth™ Characteristics

- **Unlicensed 2.4GHz radio band**
  - ISM (industrial, scientific,medical) band - **Available worldwide**
  - Also used by Microwave ovens, 802.11, HomeRF…
- **Gross data rate of 1 Mbit/s**
- **Basic 10m range extended to 100m with amplifiers**
- **TDMA - TDD - Frequency hopping**
- **Mixed voice / data paths**
- **Encryption**
- **Low power**
- **Low cost**
- **Extremely small**
- **Ubiquitous radio link**

Bluetooth™ Market Projections



	2001E	2002E	2003E	2004E	2005E	2006E
Total Bluetooth Chipsets (in millions)	48,1	207,7	492,1	921,1	1477	2216
Average Price Per Chipset (in millions of $)	8,50	5,10	4,08	3,26	2,68	2,28
Bluetooth Chip Market Revenue (in millions of $)	409	1059	2008	3006	3953	5042

Source: Merrill Lynch

Who is Bluetooth?

- **Harald Blaatand "Bluetooth" II**
- **King of Denmark 940-981**
  - Son of Gorm the Old (King of Denmark) and Thyra Danebod (daughter of King Ethelred of England)
- **This is one of two Runic stones erected in his capital city of Jelling (central Jutland)**
  - This is the front of the stone depicting the chivalry of Harald
  - Harald controlled Denmark and Norway
  - Harald thinks mobile PCs and cellular phones should seamlessly communicate

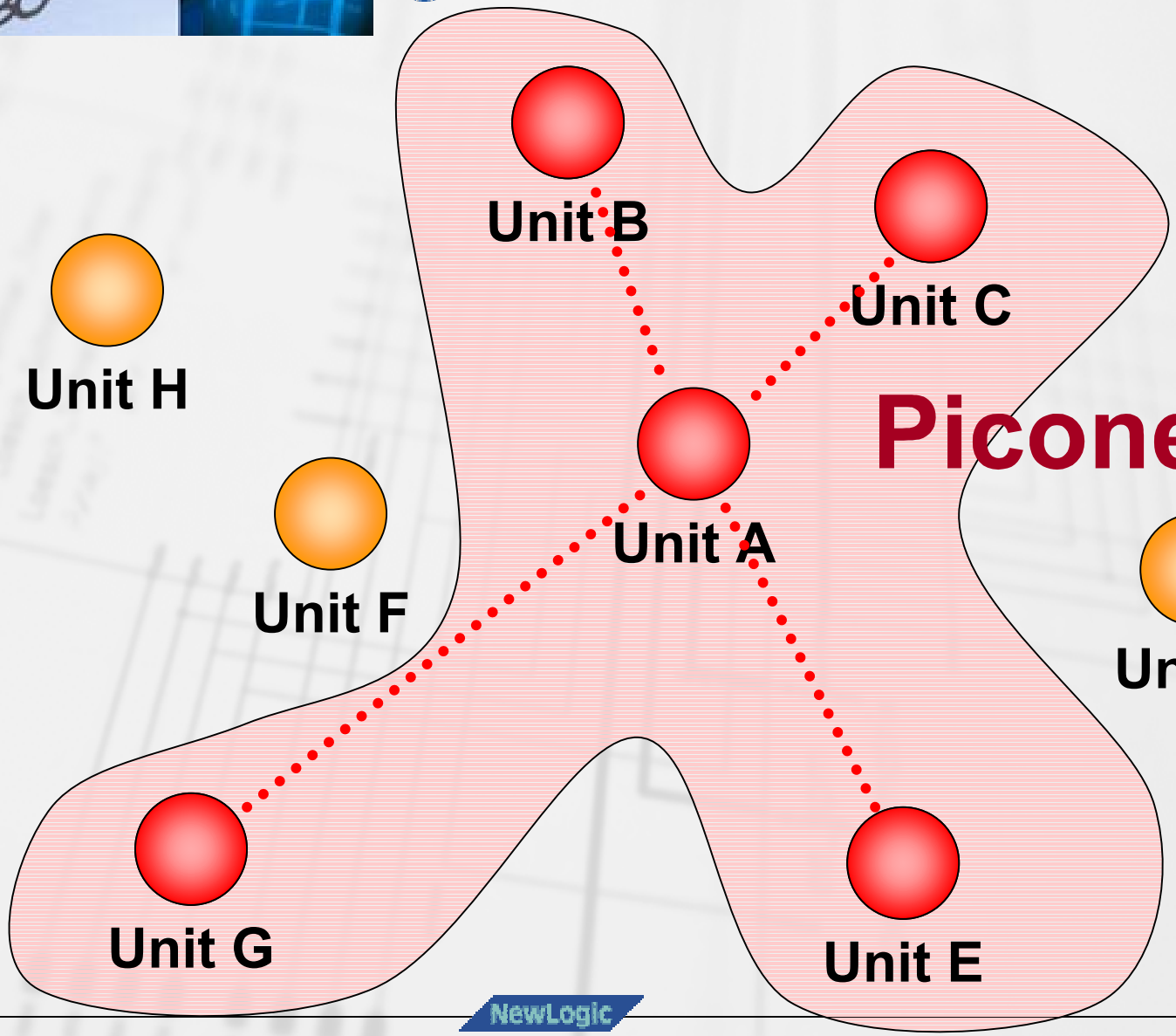
Bluetooth™ Network Topology

Bluetooth™

Tutorial

NewLogic

Bluetooth™ Piconet - 1



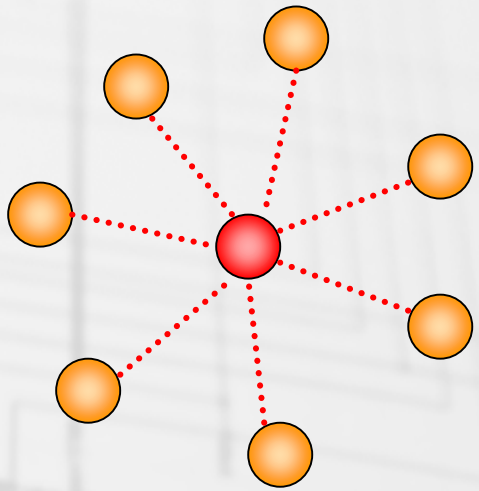
NewLogic

Bluetooth™ Piconet - 2

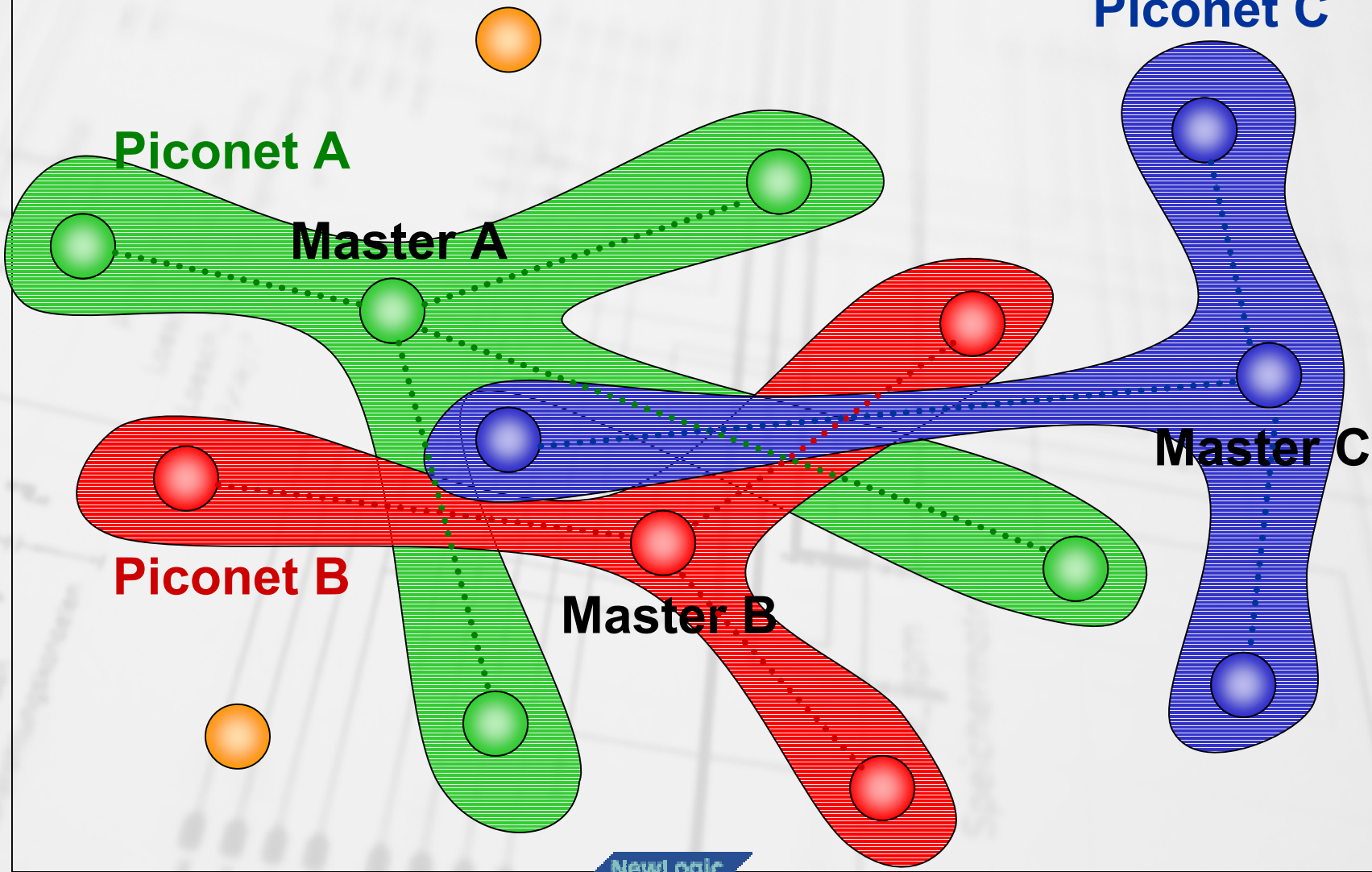
- **A piconet is characterized by the master**
  - Frequency hopping scheme
  - Access code
  - Timing synchronization
- **Master determines the bit rate allocated to each slave**
- **Slaves do not synchronize to the master**
  - Calculate offsets to master's Bluetooth clock
  - Monitor timing drift

Bluetooth™ Piconet - 3

- **Only one master**
  - Dynamically selected
  - Roles can be switched
- **Up to 7 active slaves**
  - Active piconet
- **Up to 255 parked slaves**
  - Can be reactivated quickly
- **No central network structure**
  - “Ad-hoc” network

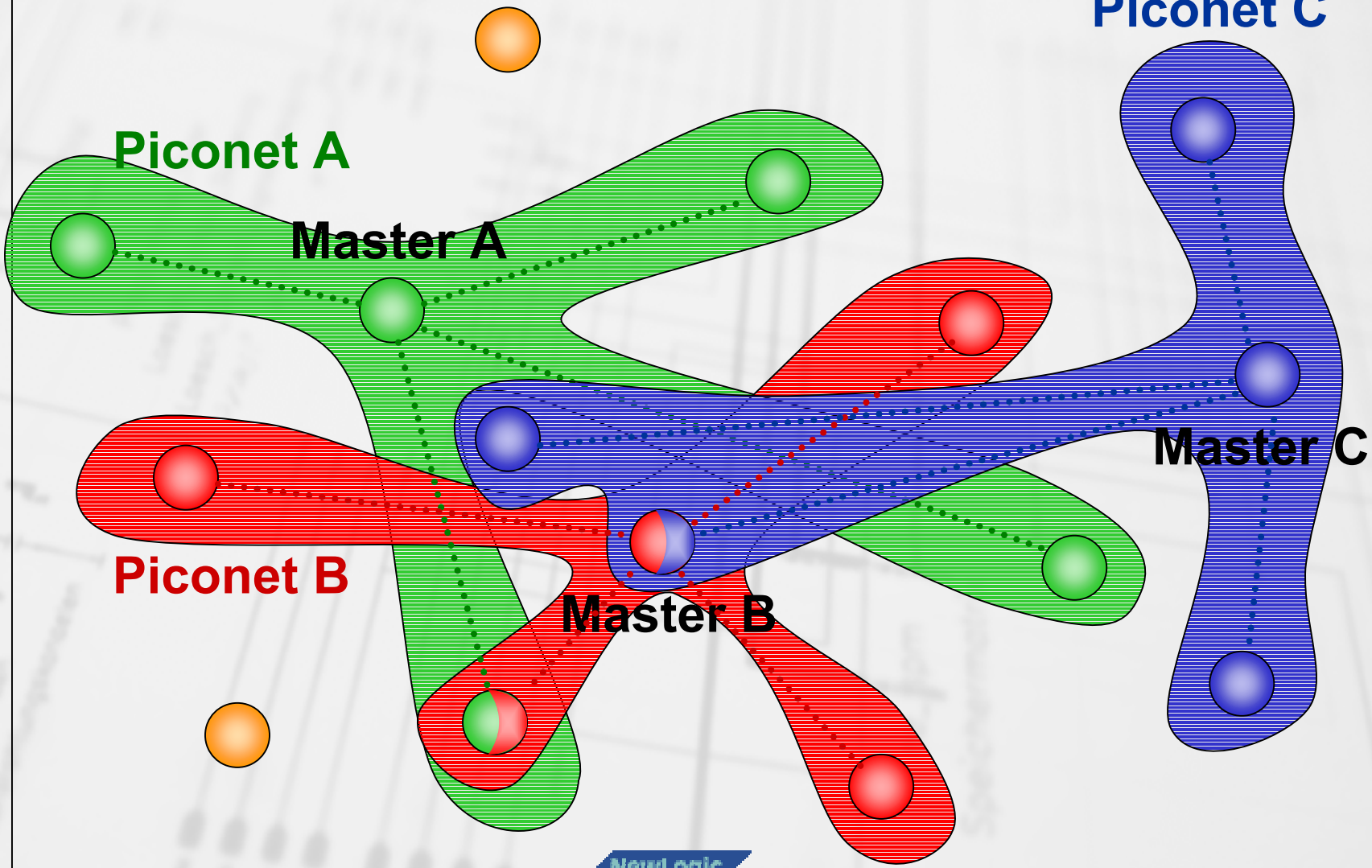


Bluetooth™ Scatternet - 1



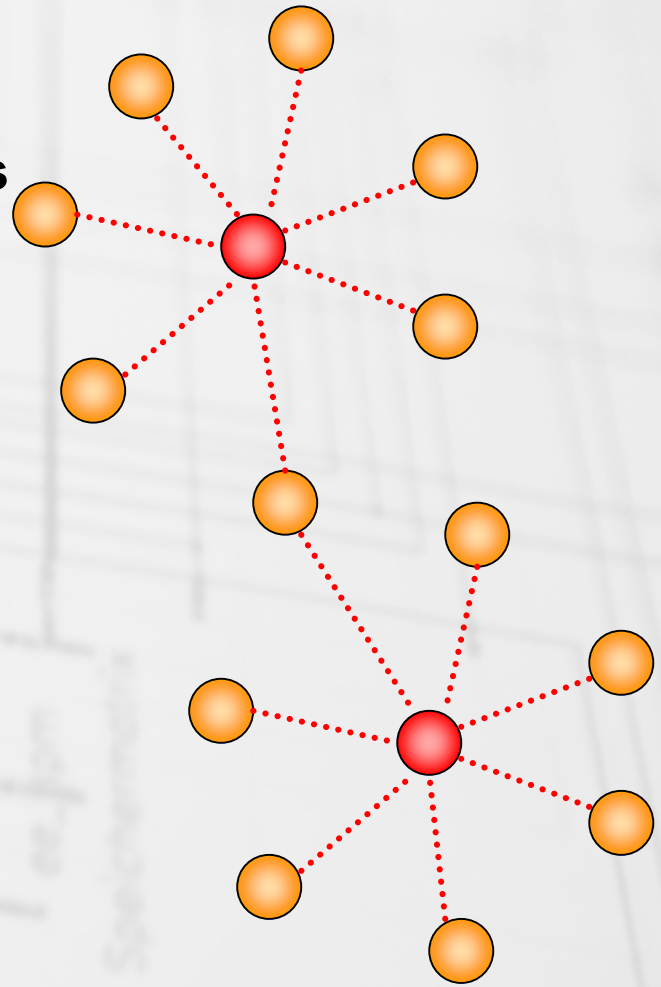
NewLogic

Bluetooth™ Scatternet - 2



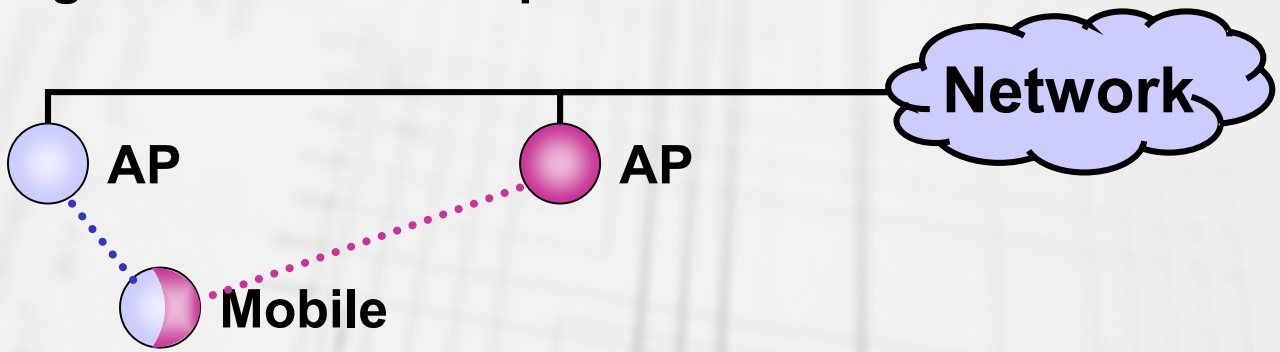
Bluetooth™ Scatternet - 3

- **Interconnected piconets**
- **One master per piconet**
- **Few devices shared between piconets**
  - Master/Slave
  - Slave/Slave
  - Need special features
- **No central network structure**
  - “Ad-hoc” network



Scatternet applications

- Roaming between access points



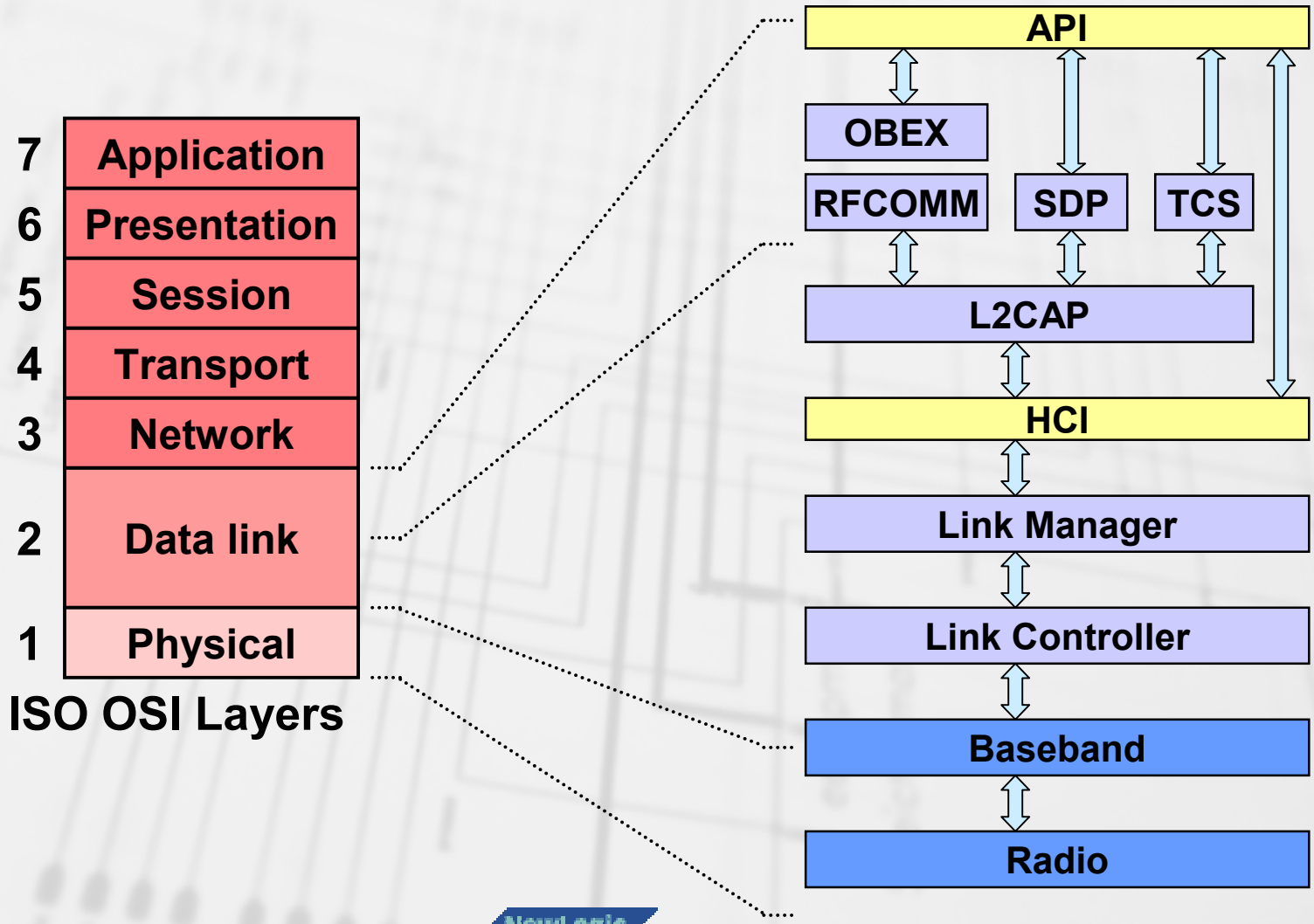
- Data exchange across piconets

Bluetooth™

Tutorial

NewLogic

Generalities on protocol stack



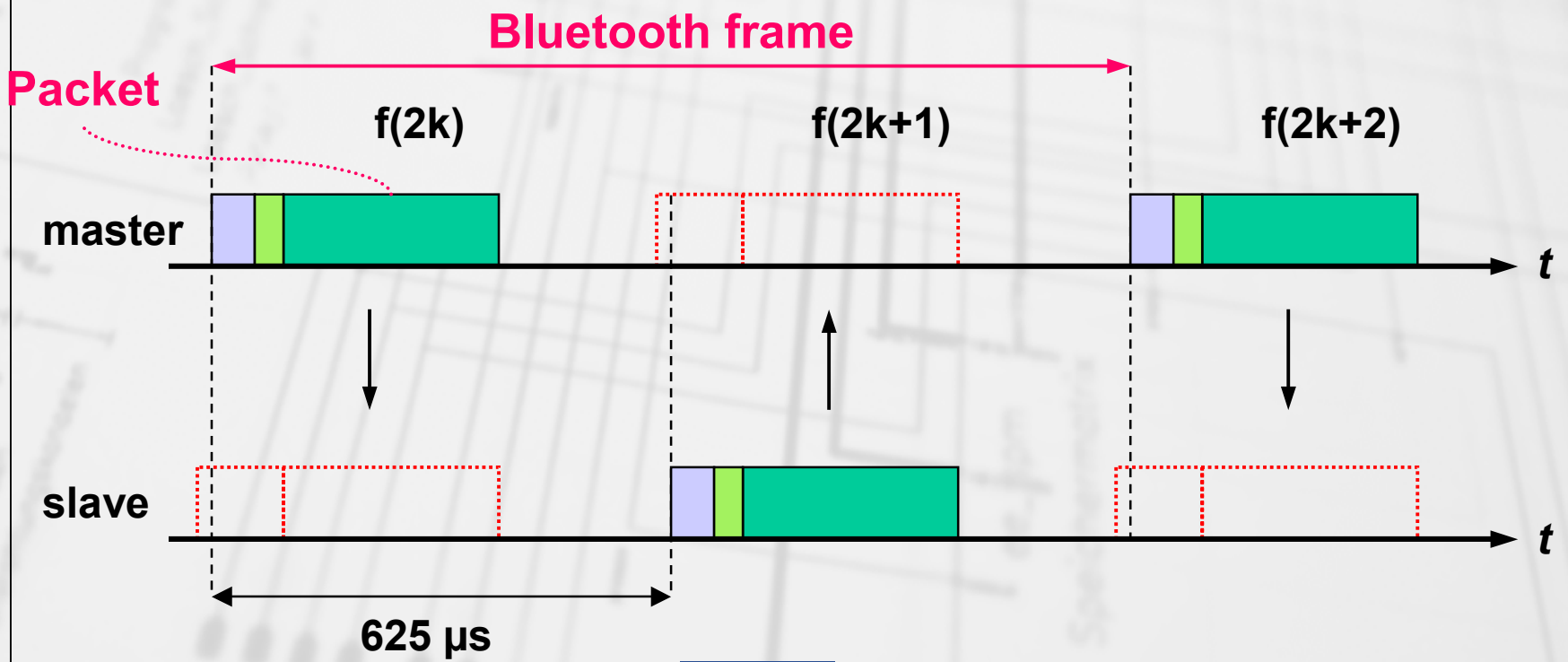
Bluetooth™ Radio - 1

- **Unlicensed 2.4GHz radio band**
  - ISM (industrial, scientific,medical) band
  - Also used by Microwave ovens, 802.11, HomeRF…
- **Fast frequency hopping**
  - 1600 (or 3200) hops/s
  - 79 frequencies
  - 1 MHz spacing
  - 220 µs switching time

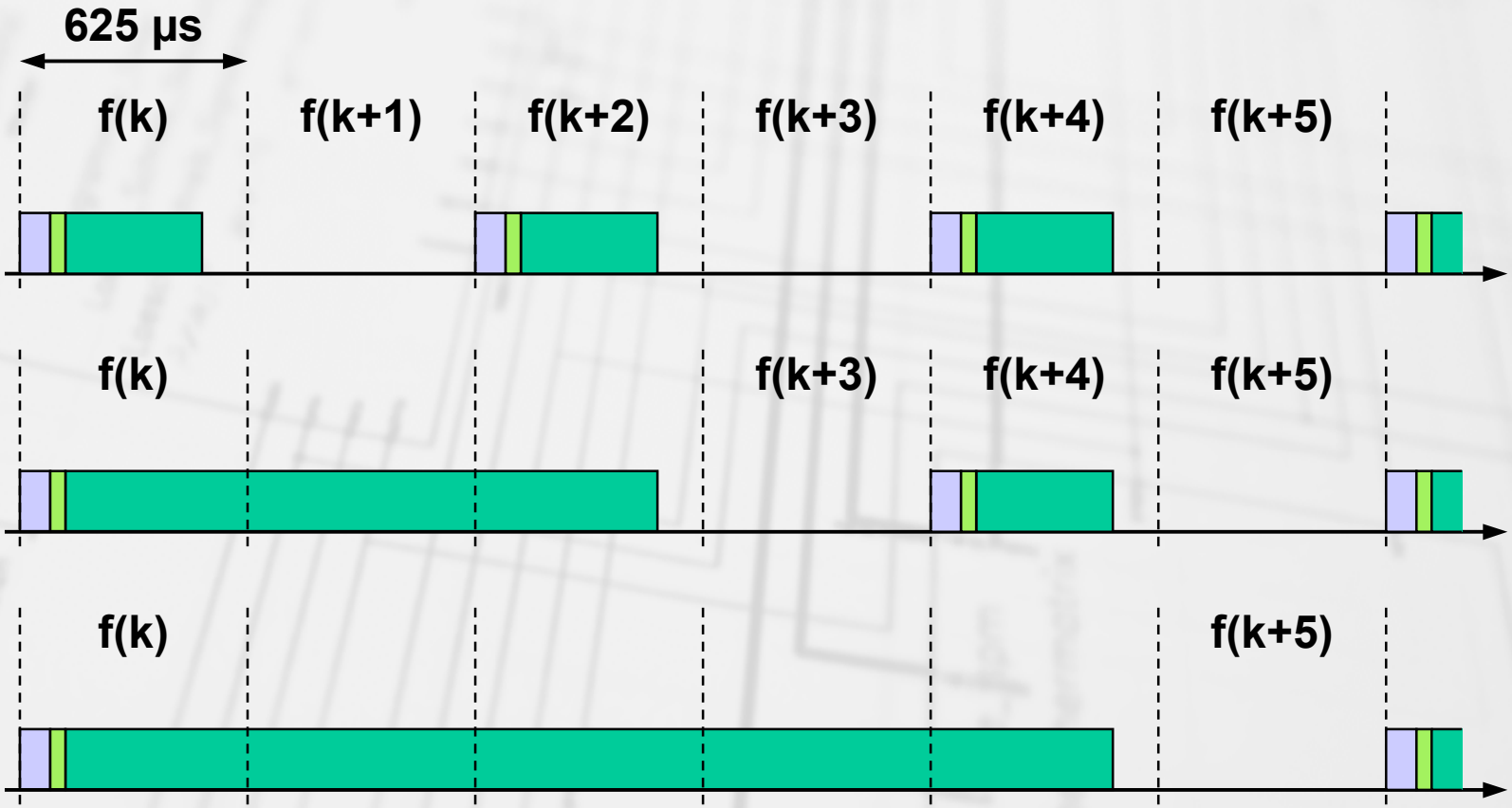
Bluetooth™ Radio - 2

- **Basic 10m range (with 0 dBm radio)**
- **Extended 100m range (20 dBm)**
- **Power classes**
  - Class 1
    - Maximum output power: 100 mW (20 dBm)
    - Minimum output power: 1 mW (0 dBm)
  - Class 2
    - Maximum output power: 2.5 mW (4 dBm)
    - Minimum output power: 0.25 mW (-6 dBm)
  - Class 3
    - Maximum output power: 1 mW (0 dBm)
- **RSSI-based power control**

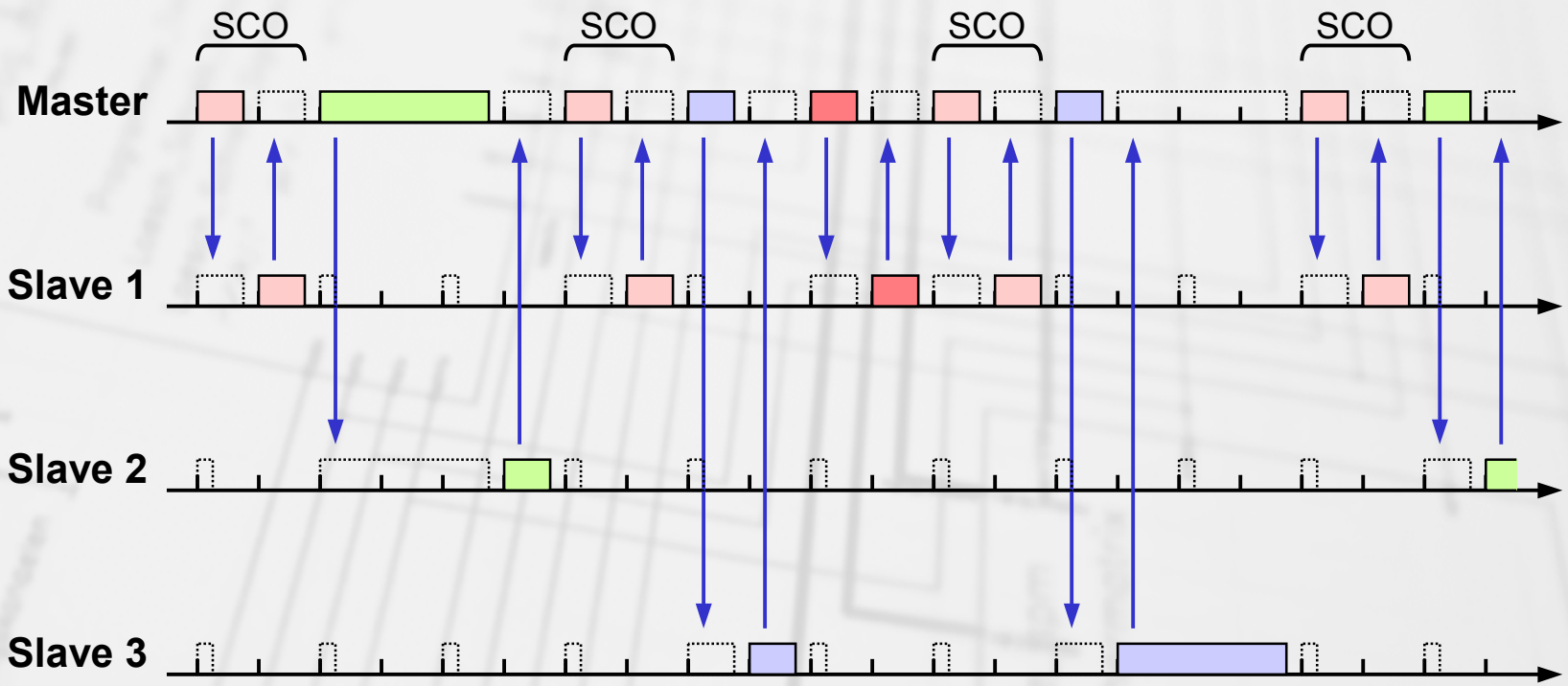
- TDMA – Time division multiple access
- TDD – Time division duplex



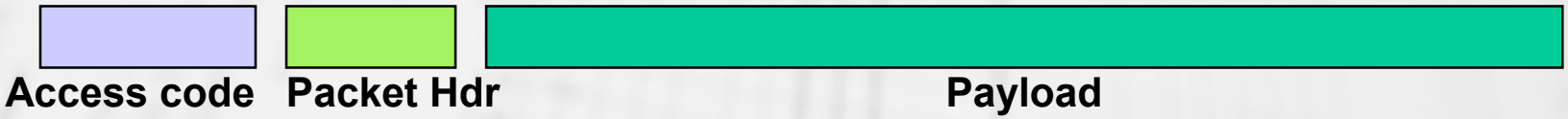
- Multi-slot Packets



Bluetooth™ Baseband - 3



- **Packet format**



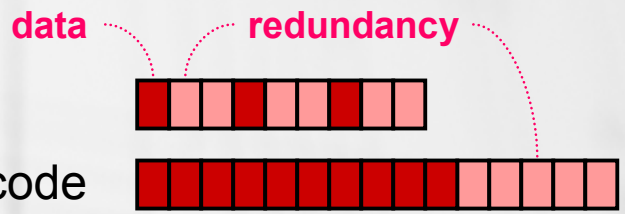
- **Packet types**
  - HV1, HV2, HV3 - Voice packets
  - DV - Mixed voice/data
  - DM1, DM3, DM5 - Protected data packets
  - AUX1, DH1, DH3, DH5 - Unprotected data packets
  - NULL, POLL, ID, FHS - Baseband control packets

Bluetooth™ Baseband - 5

- Data rates

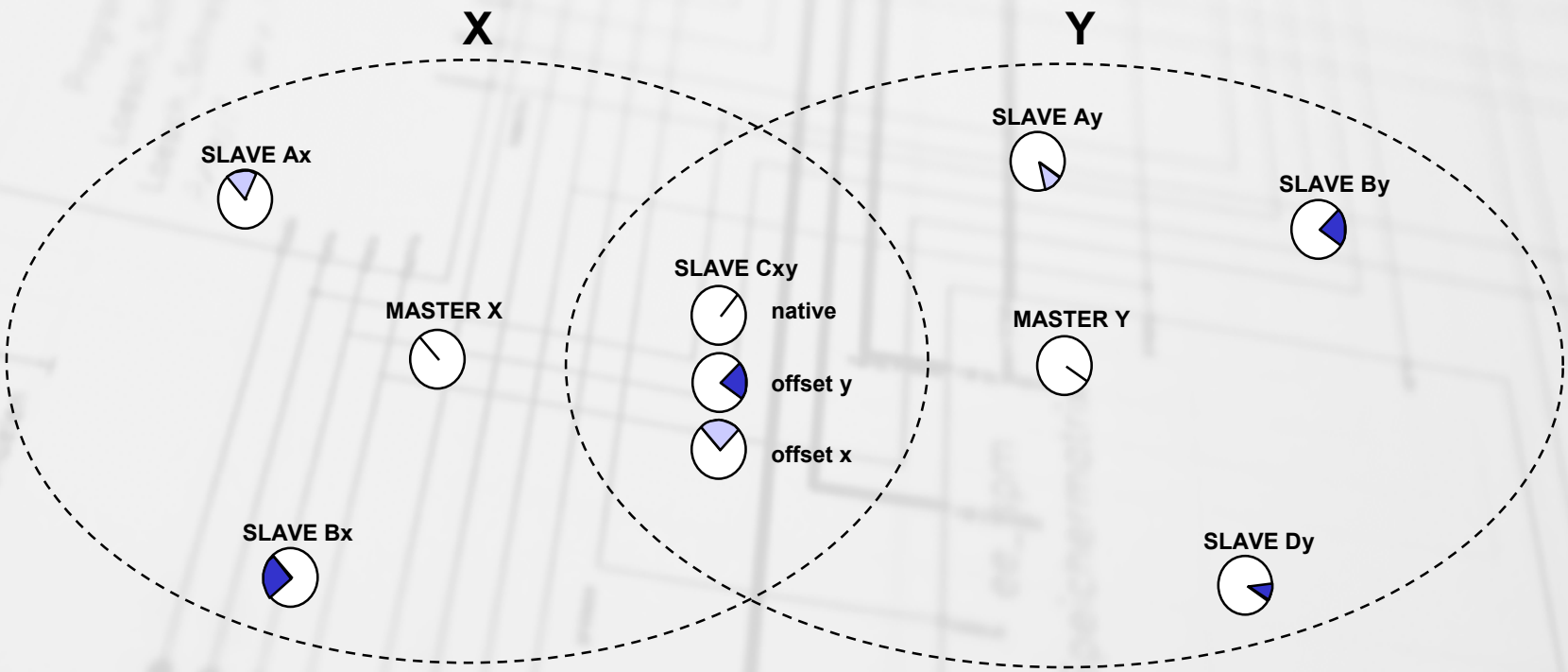
Packet type	FEC	Symmetric max rate (kb/s)	Asymmetric max rate (kb/s)	
DM1	2/3	108.8	108.8	108.8
DH1	no	172.8	172.8	172.8
DM3	2/3	258.1	387.2	54.4
DH3	no	390.4	585.6	86.4
DM5	2/3	286.7	477.8	36.3
DH5	no	433.9	723.2	57.6
AUX1	no	185.6	185.6	185.6

- **Data error protection**
  - FEC (Forward Error Correction)
    - 1/3 FEC - Repeat each bit 3 times
    - 2/3 FEC - (15,10) shortened Hamming code
  - ARQ (Automatic Repeat Request)
    - Unnumbered
  - CRC (Cyclic Redundancy Check)
    - HEC (Header Error Check)
    - Payload CRC
- **Encryption**
- **Whitening**



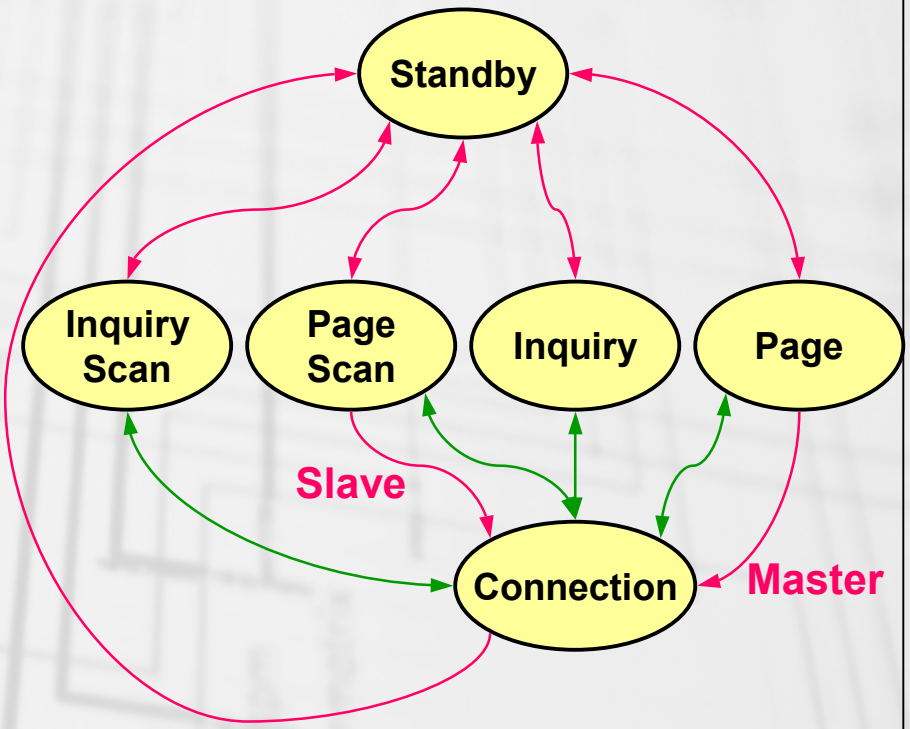
- **Bluetooth native clock**
  - 3.2 kHz (312.5 µs period) - 25 ppm
  - 28-bit free running counter (~ 1 day period)
  - Never resynchronized
- **Estimated clock for paging**
- **Piconet clock**
  - Native clock of the master
  - Slaves maintain a relative offset to their native clocks
  - Drift compensation necessary

- **Scatternet case**
  - Master/Slave units use 1 offset
  - Slave/Slave units use 2 offsets

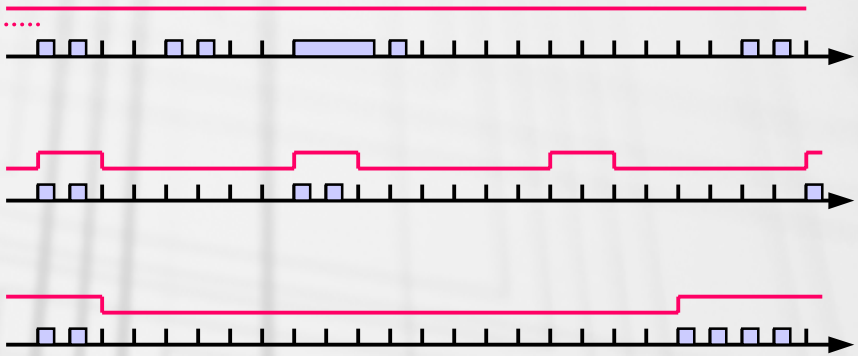


Bluetooth™ Link Controller - 1

- **Standby**
  - Device powered on
- **Inquiry**
  - Discover devices in the area
  - Collect addresses
- **Page**
  - Connect to a specific device
- **Inquiry scan**
  - Discoverable state
- **Page scan**
  - Device waiting to join a piconet
- **Connection**
  - Actively on a piconet
  - Master or slave



- **Modes in connection state**
  - Active
    - Maximum 7 slaves
  - Sniff
    - Low-power active mode
  - Hold
    - One-time interval
  - Park
    - Virtually unlimited number of slaves
    - Beacon
    - Broadcast communication



Bluetooth™ Link Controller - 3

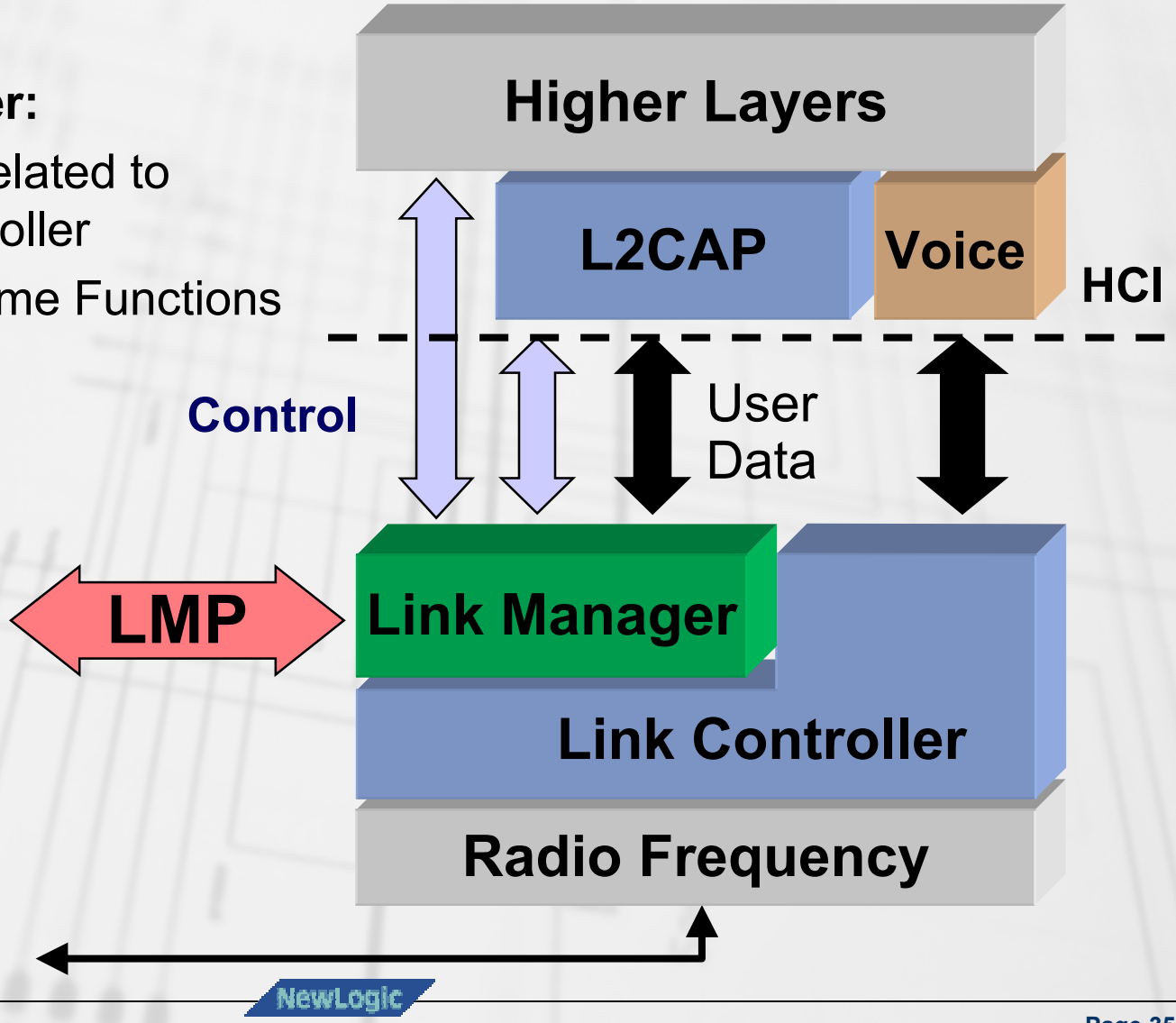
- **Synchronous Connection-Oriented (SCO) Link**
  - Circuit switching
  - Symmetric, synchronous services
  - Slot reservation at fixed intervals
- **Asynchronous Connection-Less (ACL) Link**
  - Packet switching
  - (A)symmetric, asynchronous services
  - Polling access scheme

Bluetooth™ Link Controller - 4

- **Logical channels**
  - Control channels:
    - **LC** link control
    - **LM** link manager
  - Traffic channels:
    - **US** synchronous user data
    - **UA** asynchronous user data
    - **UI** isochronous user data
- **Channel mapping**
  - Packet header:
    - LC
  - Packet payload:
    - LM, US, UA, UI

Bluetooth Link Manager - 1

- **Link Manager:**
  - Closely Related to Link Controller
  - No Real-time Functions

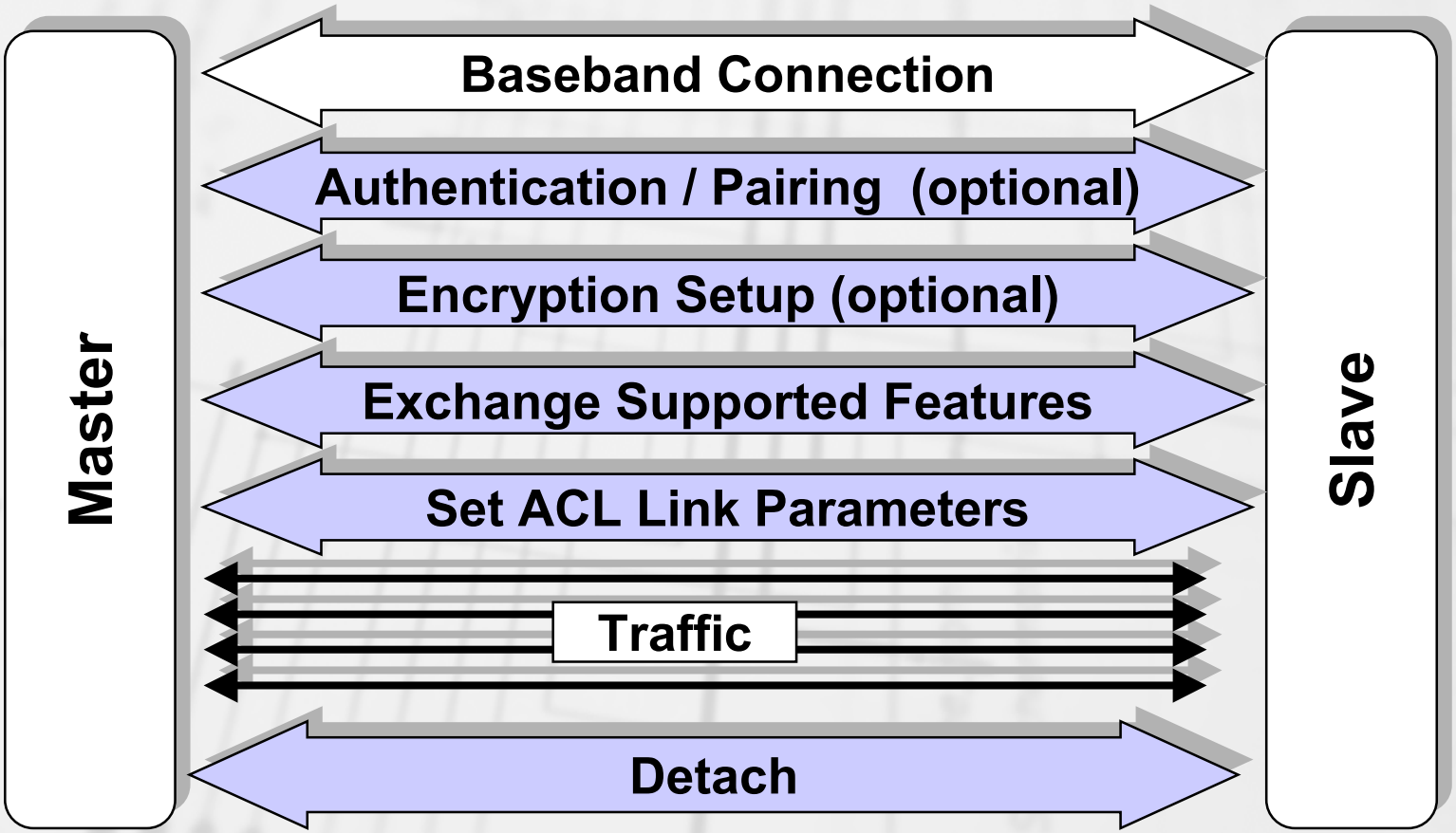


Bluetooth™ Link Manager - 2

- **Piconet management**
  - Attach and detach slaves
  - Master-slave switch
  - Establishing ACL and SCO links
  - Handling of low power modes: Hold, Sniff, Park
- **Link configuration**
  - Supported features
  - Quality of Service, usable packet types
  - Power Control
- **Security management**
  - Authentication
  - Encryption including key management

Bluetooth Link Manager - 3

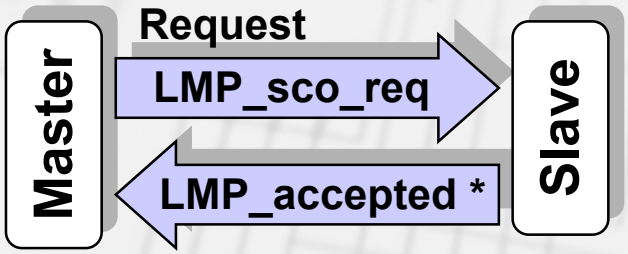
- ACL Link Setup and Removal



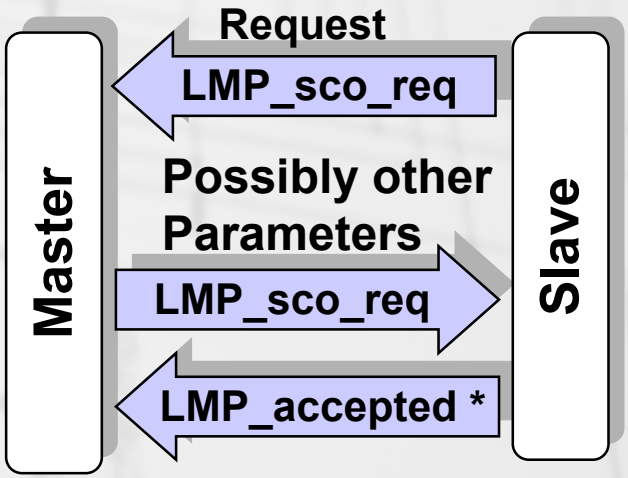
Bluetooth Link Manager - 4

- SCO Link Setup and Removal
- Setup Negotiation

1. Master-initiated

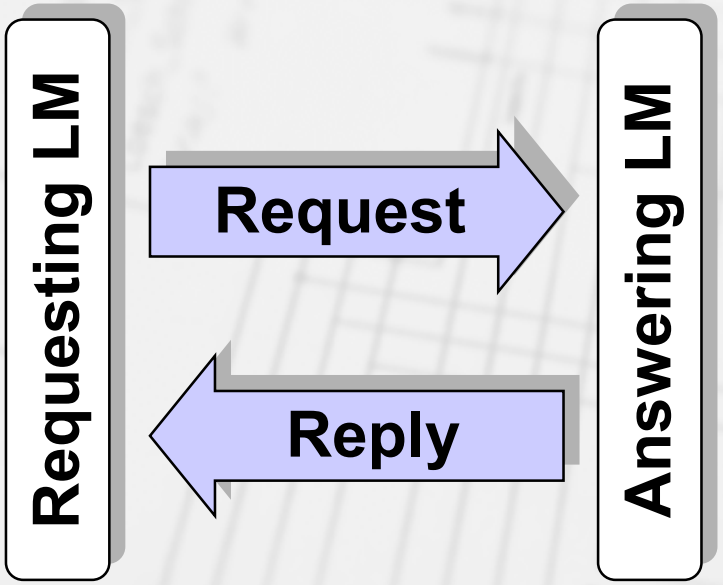


2. Slave-initiated



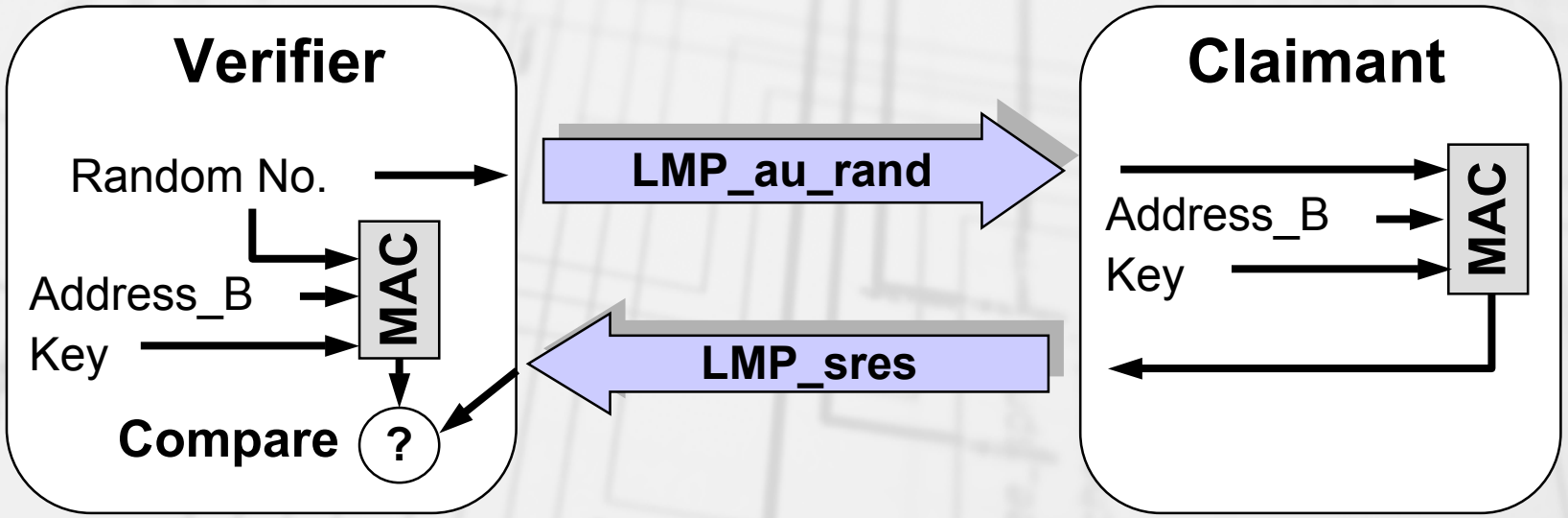
* or LMP_not_accepted

Requesting information on Remote Device

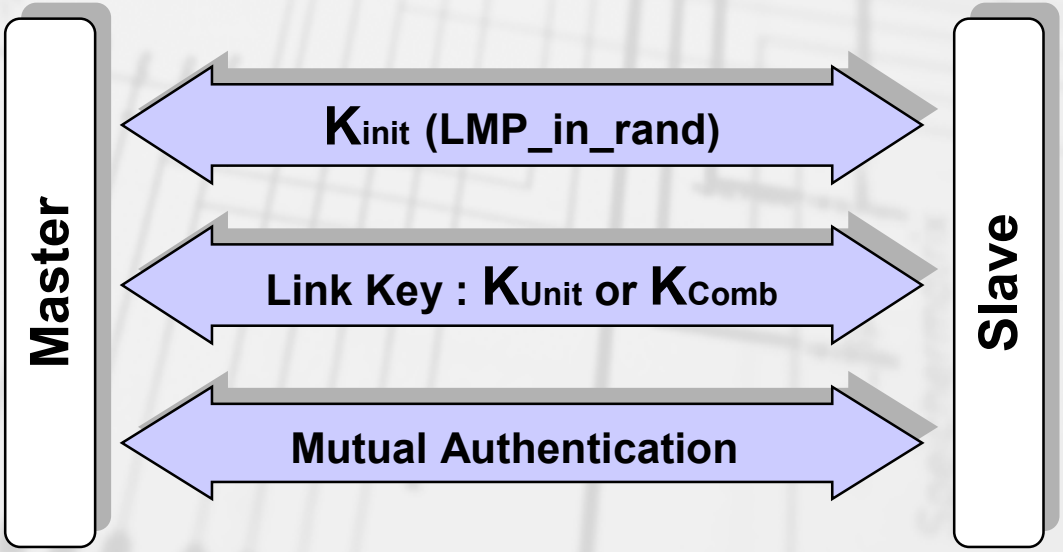


- **Link Information Commands**
  - LMP Version
  - Supported Features
    - Packet Types
    - Low Power Modes
    - Master-Slave Switch
    - Power Control
    - SCO Air Mode Parameters
    - L2CAP
    - Encryption
  - Timing Accuracy
  - Clock Offset
  - Name of Device

- **Security (1): Authentication**
  - Challenge Response Scheme (ISO/IEC 9798-2)
  - 32 Bit - Authentication Code (MAC)
  - Authentication of Master, Slave or both

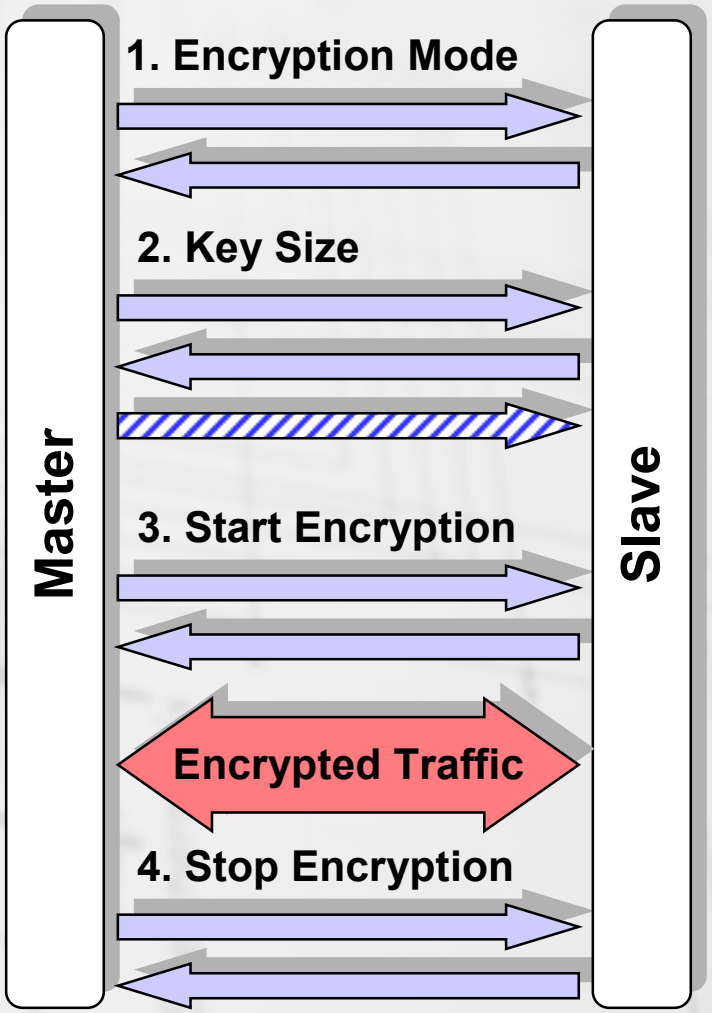


- **Security (2): Pairing**
  - Authentication requires a common secret key
  - Pairing includes:
    - Generation of Initialization Key
    - Generation of Link Key
    - Mutual Authentication



Bluetooth™ Link Manager - 8

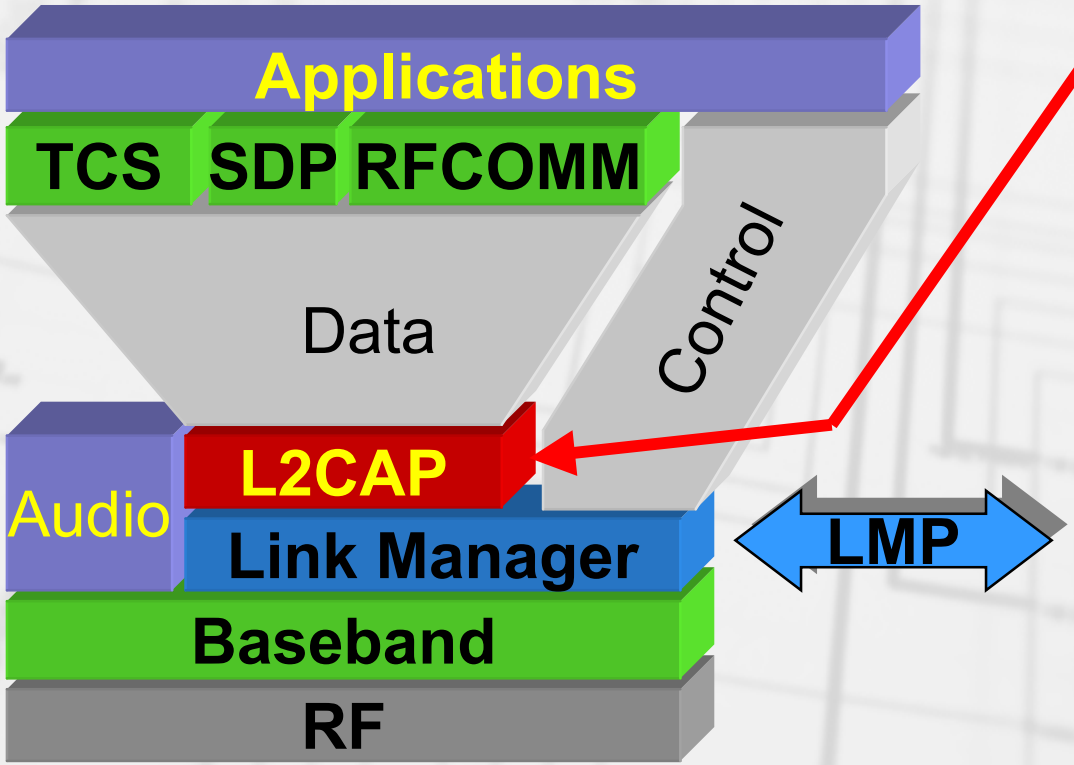
- **Security (3): Encryption**
  - Prerequisites
    - Successful authentication (at least one direction)
    - Common Link Key available
  - Negotiation in 3 Steps:
    - Using encryption
      - (Point-to-Point / Broadcast)
    - Key size:
      - Regulations may occur
      - Negotiation based on preferred and allowed key length
    - Start encryption



Bluetooth™ Link Manager - 9

- **Security (4): Key Generation**
  - Options for Keys
    - Unit Key from Master or Slave
    - Combination Key: calculated from random numbers (secure exchange)
    - Temporary Key
  - Temporary and combination keys can be changed at any time

What is L2CAP?



Bluetooth™ L2CAP - 2

- **Logical Link Control and adaptation Protocol (L2CAP)**

- **Protocol Multiplexing**
  - Goal: Pass packets used by a particular network protocol to the appropriate handler
- **Segmentation and Reassembly (SAR)**
  - Goal: Hide data link packet lengths from network-layer protocols
- **Quality of Service**
  - Goal: Negotiate and enforce QoS contracts

Bluetooth L2CAP - 3

- **Protocol Architecture**
  - Connection-oriented
    - Channel identifier used to label each connection
    - Channel is assumed to be full-duplex
    - QoS flow specification assigned to each channel direction
  - Datagram-based, no Streams
    - Packet boundaries are preserved
    - L2CAP does NOT perform retransmission
    - L2CAP does NOT perform Flow Control

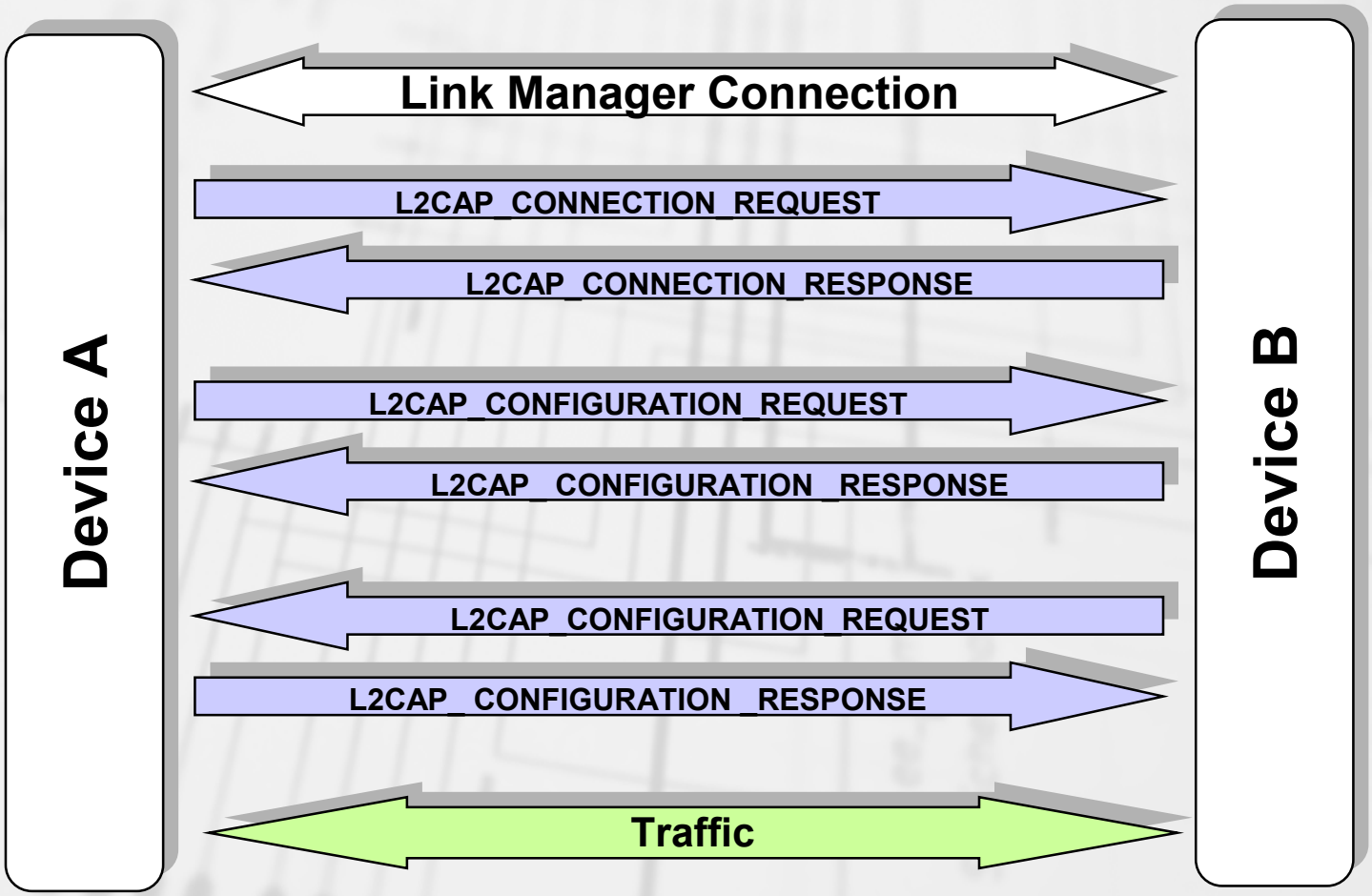
Bluetooth L2CAP - 4

- **L2CAP Packet Format**

Length (16 bits)	DCID (16 bits)	Payload (0-65535 bytes)

  - Length
    - Specifies the length of the payload in bytes
  - Destination Channel ID (DCID)
    - Identifies the channel to which the packet will be delivered
  - Payload
    - Data received from and sent to the network layer
    - Maximum transmission unit (MTU) limits payload sizes

- L2CAP Channel Establishment

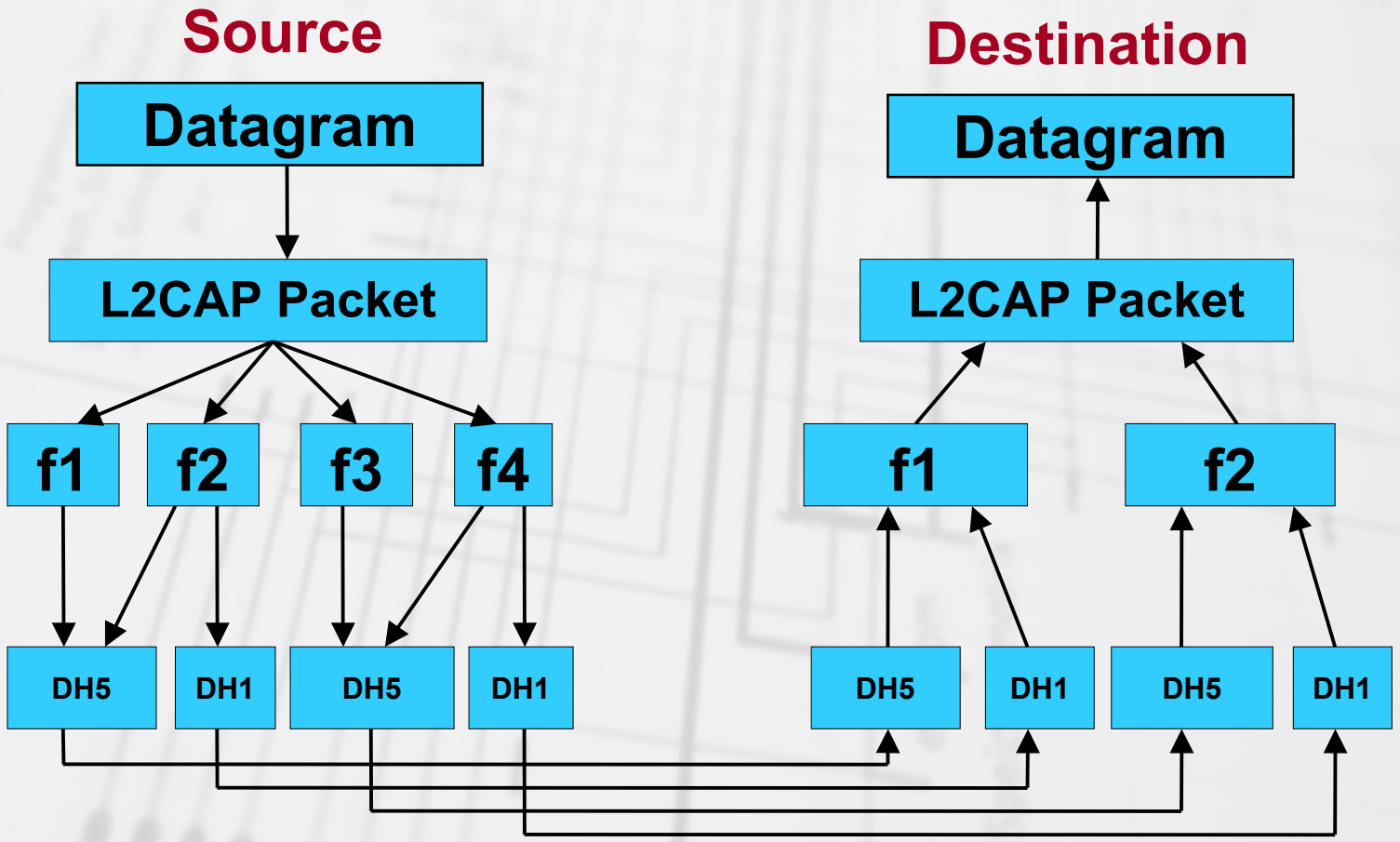


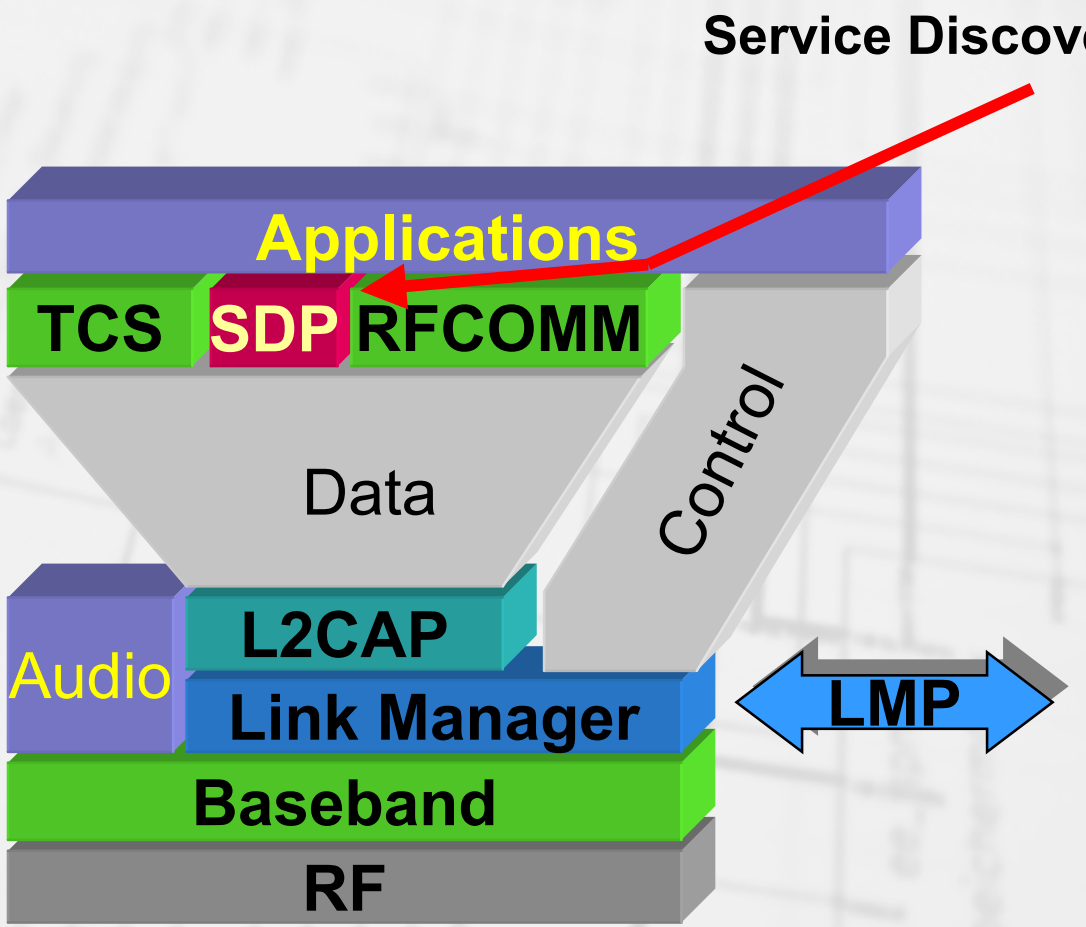
- **Segmentation and Reassembly (SAR)**
  - Use logical channel information from Baseband
    - LCH=10 implies start of an L2CAP packet
    - LCH=01 implies continuation of L2CAP packet

L2CAP packet

Baseband packet

- SAR Example

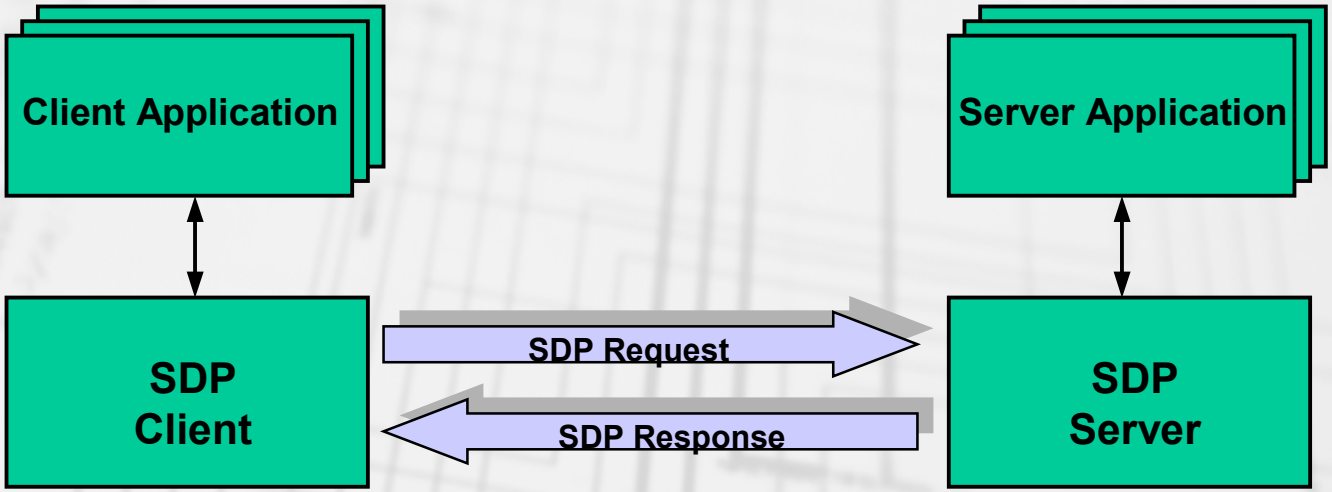

Source
Destination
Datagram
L2CAP Packet
f1
f2
f3
f4
DH5
DH1
DH5
DH1
Datagram
L2CAP Packet
f1
f2
DH5
DH1
DH5
DH1


Service Discovery Protocol
Applications
TCS
SDP
RFCOMM
Data
Control
Audio
L2CAP
Link Manager
LMP
Baseband
RF

Bluetooth SDP - 2

- **Protocol Architecture**
  - Connectionless - Client/Server
  - SDP defines How services are represented in the DB
    - Server database describes all the services available on a device (Service records)
  - SDP defines How to access to the server DB information

- **SDP Client/Server Model**
  - Transaction identifier used to label each SDP transaction



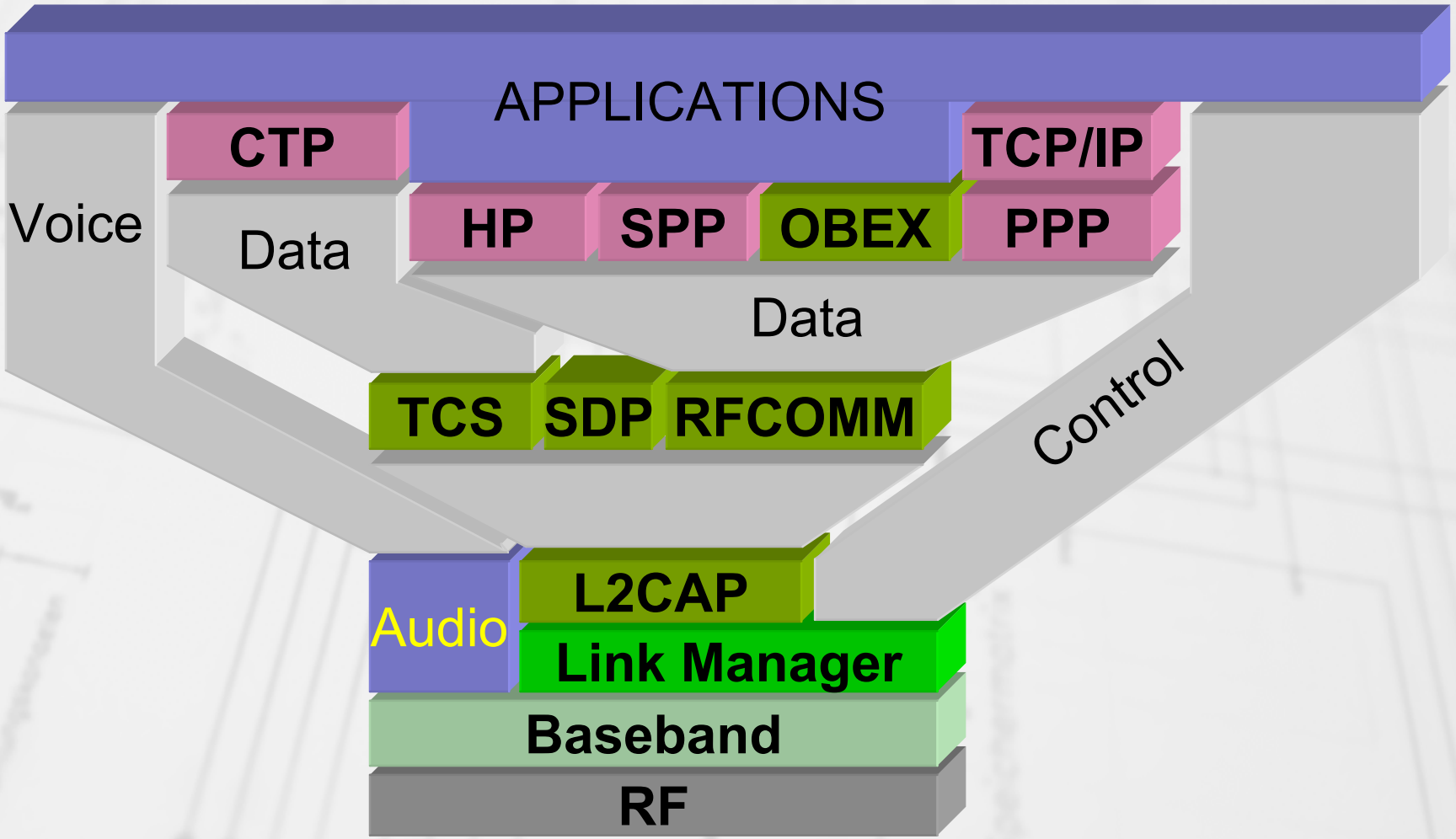
- **Protocol Data Unit Format**

PDU id (1 bytes)	Transaction Id (1 bytes)	Parameter Length (2 bytes)	Parameter 1-N (Parameter Length bytes)

Bluetooth SDP - 4

- **Service Discovery**
  - Searching for Services
    - What are the Services provided by the remote device ?
      - IrDA-like printer
      - Headset
      - AudioGateway
      - …
  - Browsing for Services
    - What are the Service Attributes ?
      - e.g. : (L2CAP, PSM=RFCOMM), (RFCOMM, CN=1), (PostscriptStream)
  - Accessing to the Services (not in the scope of SDP)

Bluetooth™ Applications - 1



Bluetooth™ Applications - 2

- CTP : Cordless Telephony Profile
- HP : Headset Profile
- SPP : Serial Port Profile
- PPP : Point To Point Protocol
- OBEX : Object Exchange Protocol

Bluetooth™ Implementation

Bluetooth™

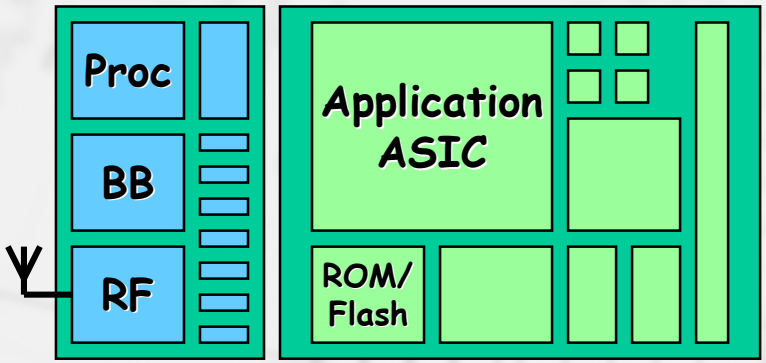
Tutorial

NewLogic

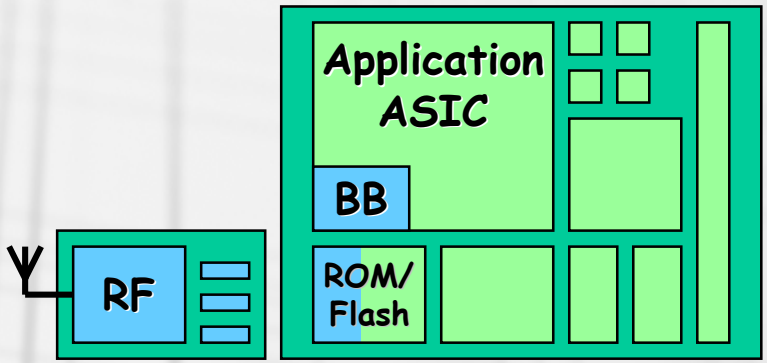
Implementation choices

- **Trade-offs** (Flexibility, cost, performance, size, power consumption)

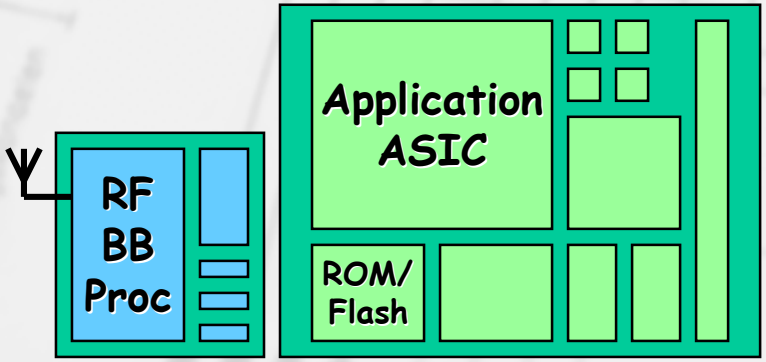
Bluetooth module



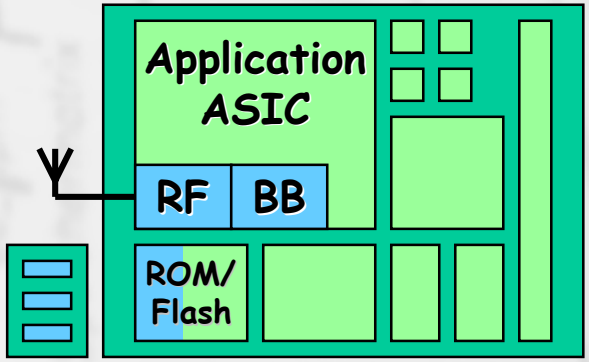
Bluetooth IP + Bluetooth RF



Bluetooth single chip

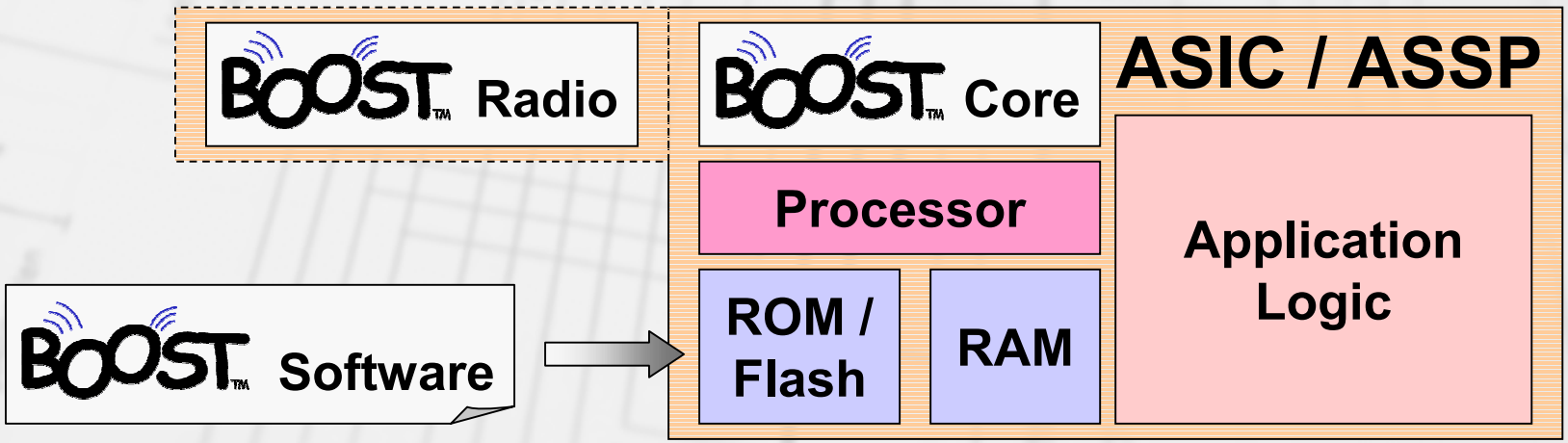


Bluetooth IP + RF IP



Integration example

- **BOOST integrated approach**
  - Bluetooth radio
  - Bluetooth baseband core
  - Bluetooth software stack



Bluetooth™ Live Demo

Bluetooth™

Tutorial

Bluetooth™ References

Bluetooth™

Tutorial

NewLogic

Bluetooth References

- **http://www.bluetooth.com** - Bluetooth specifications online
- **http://www.newlogic.com**
- **Books:**
  - **Bluetooth: Connect without Cables** - Jennifer Bray & Charles Sturman
  - **Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications** - Brent A. Miller,Chatschik Bisdikian