بسم الله الرحمن الرحیم

Mobile Networking

Mohammad Hossein Manshaei

manshaei@gmail.com

1393

IEEE 802.15 and IEEE 802.16

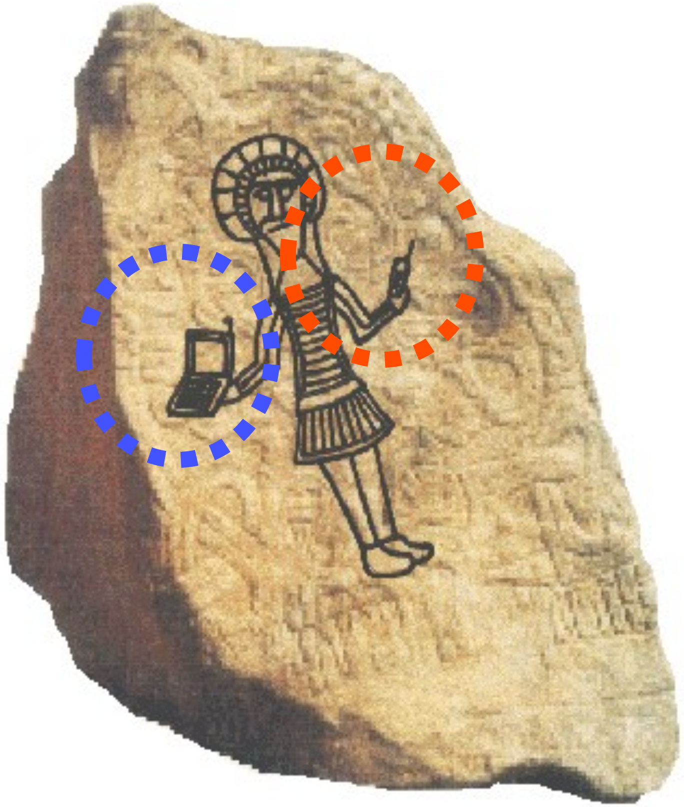
Bluetooth and WiMax

Contents

- Bluetooth
  - History and Introduction
  - IEEE 802.15.1
    - Application, Frequency, Architecture, and Protocol Stack
  - IEEE 802.15.3
  - IEEE 802.15.4
- IEEE 802.16: (Worldwide Interoperability for Microwave Access) WiMax

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)

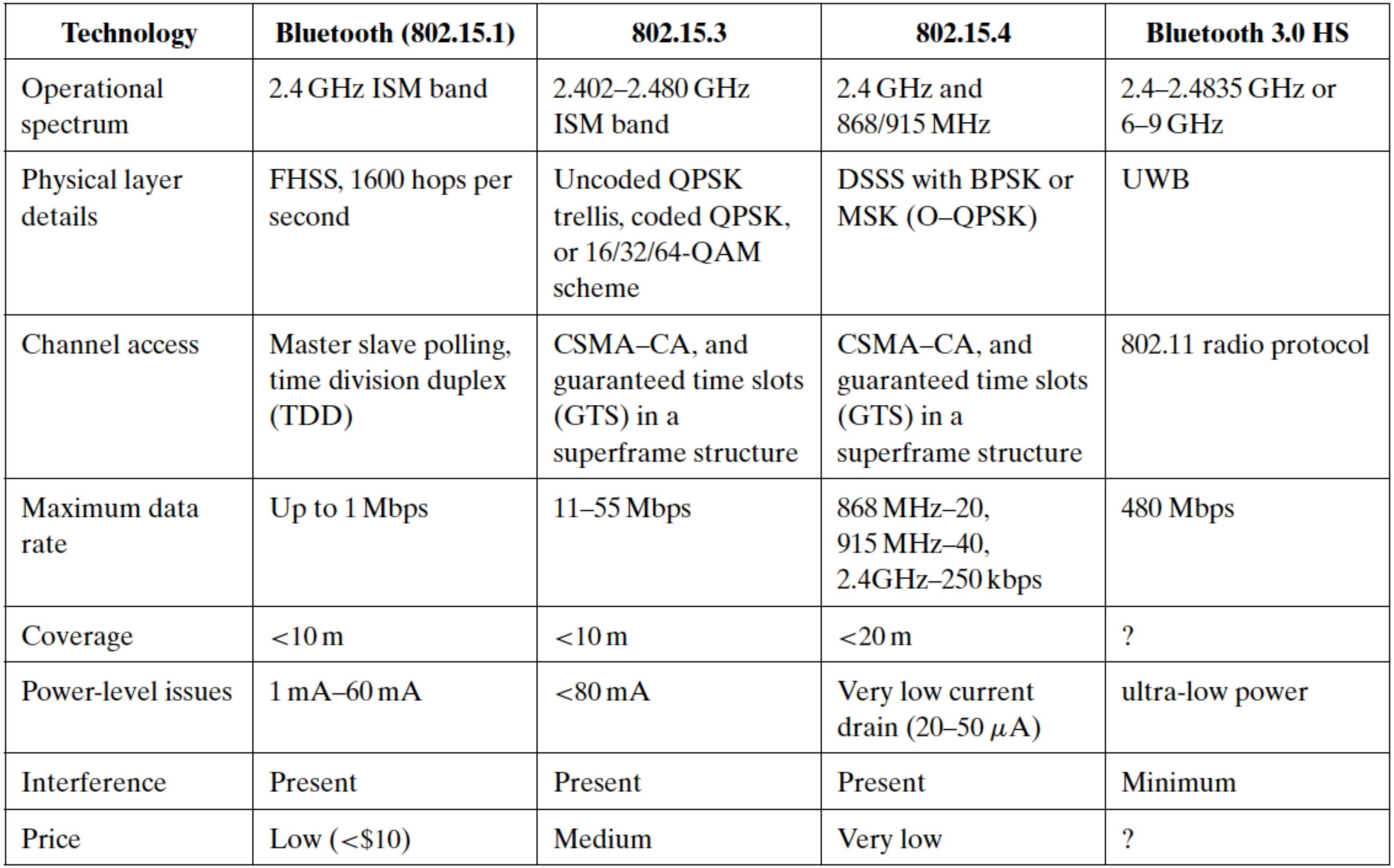


- ❑ **This is one of two Runic stones erected in his capitol city of Jelling (central Jutland)**
- ❑ The stone's inscription ("runes") say:
  - ❑ Harald controlled Denmark and Norway
  - ❑ Harald thinks "notebooks" and "cellular phones" should seamlessly communicate

Bluetooth History

- ➢ 1997 - Designed by **Ericsson**
- ➢ 1998.2 - Established the Special interest group (form SIG 1)
  Ericsson, Nokia, IBM, Toshiba, Intel
- ➢ 1998.5 - Bluetooth **Consortium** is established formally.
- ➢ 1999.7 - Bluetooth **v1.0beta** Core Specification and Foundation Profile
- ➢ 1999.12 - **Lucent**、**3Com**、**Motorola**、**Microsoft** (form SIG 2)
- ➢ **2001.2 - Bluetooth v1.1**
- ➢ 2002 – **IEEE 802.15 WPAN**
  - ◆ IEEE 802.15.1 Wireless Personal Area Networks (Bluetooth)
  - ◆ IEEE 802.15.2 Coexistence
  - ◆ IEEE 802.15.3 WPAN Higher Rate
  - ◆ IEEE 802.15.4 WPAN Low Rate

IEEE Working Groups



Technology	Bluetooth (802.15.1)	802.15.3	802.15.4	Bluetooth 3.0 HS
Operational spectrum	2.4 GHz ISM band	2.402–2.480 GHz ISM band	2.4 GHz and 868/915 MHz	2.4–2.4835 GHz or 6–9 GHz
Physical layer details	FHSS, 1600 hops per second	Uncoded QPSK trellis, coded QPSK, or 16/32/64-QAM scheme	DSSS with BPSK or MSK (O–QPSK)	UWB
Channel access	Master slave polling, time division duplex (TDD)	CSMA–CA, and guaranteed time slots (GTS) in a superframe structure	CSMA–CA, and guaranteed time slots (GTS) in a superframe structure	802.11 radio protocol
Maximum data rate	Up to 1 Mbps	11–55 Mbps	868 MHz–20, 915 MHz–40, 2.4GHz–250 kbps	480 Mbps
Coverage	<10 m	<10 m	<20 m	?
Power-level issues	1 mA–60 mA	<80 mA	Very low current drain (20–50 μA)	ultra-low power
Interference	Present	Present	Present	Minimum
Price	Low (<$10)	Medium	Very low	?

Contents

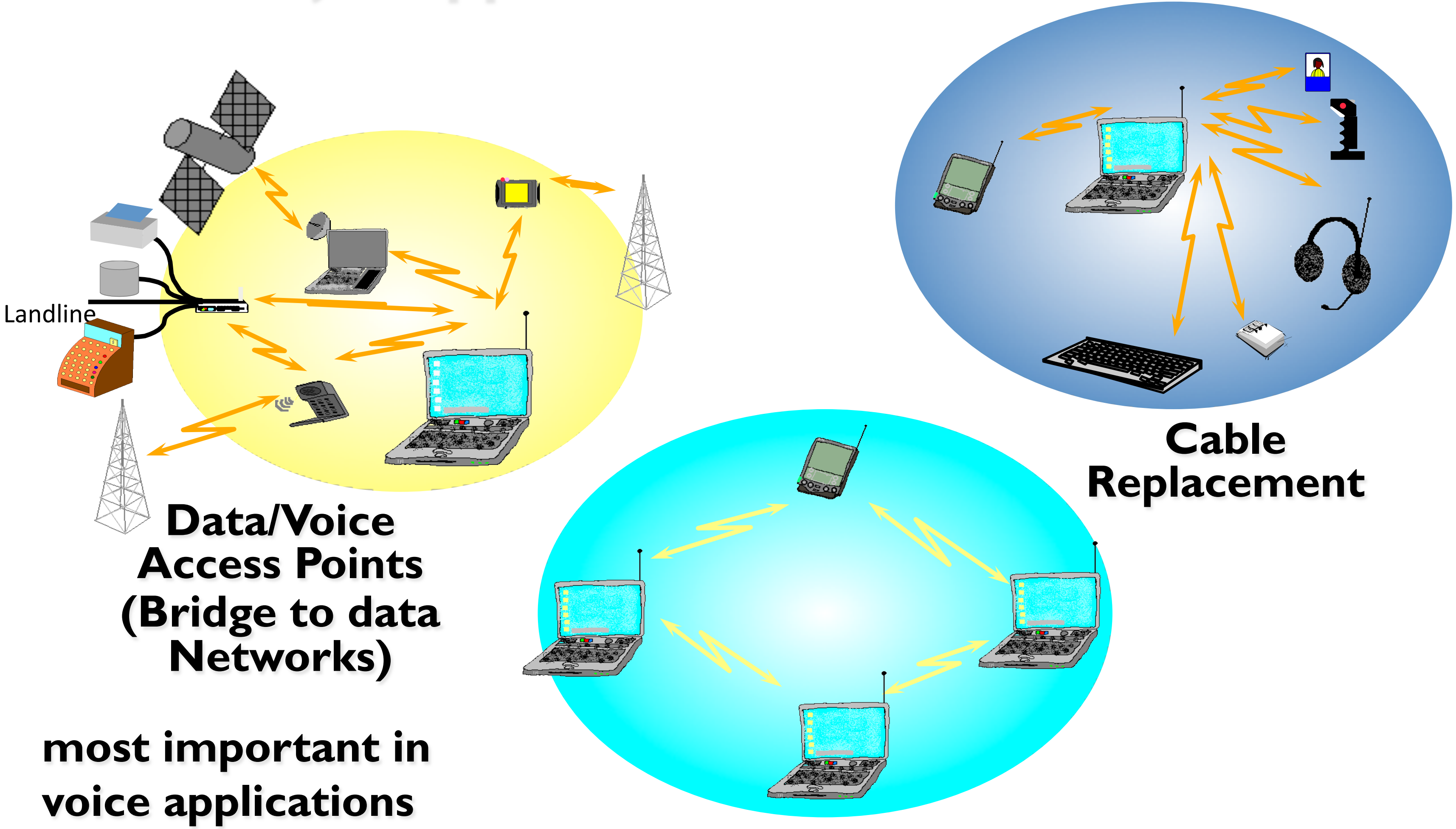
- Bluetooth
  - History and Introduction
  - IEEE 802.15.1
    - Application, Frequency, Architecture, and Protocol Stack
  - IEEE 802.15.3
  - IEEE 802.15.4
- IEEE 802.16: (Worldwide Interoperability for Microwave Access) WiMax

History and Technology

IEEE 802.15.1 (Bluetooth)

What does Bluetooth do?

- ♦ Three major applications



Data/Voice Access Points (Bridge to data Networks)

most important in voice applications

Cable Replacement

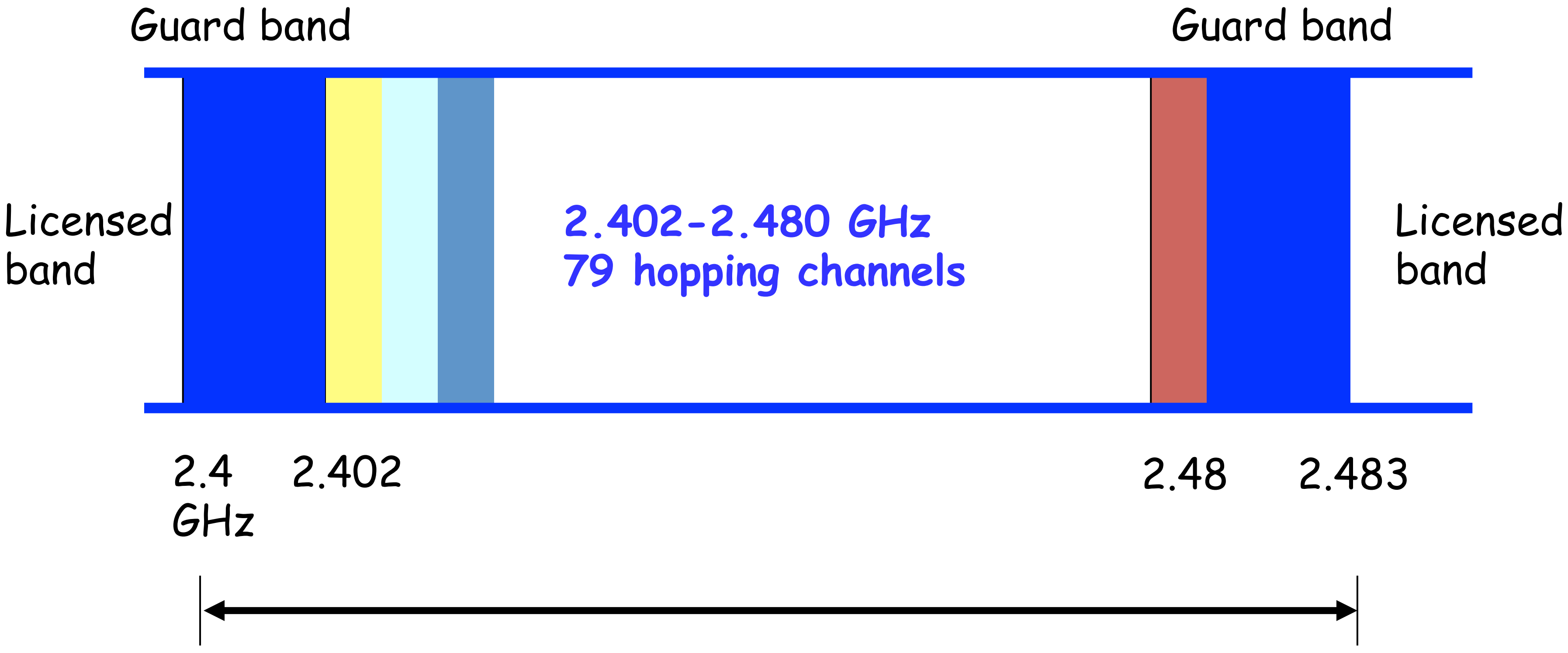
Personal Ad-hoc Networks

Key Characteristics of Bluetooth

- Low cost
  - Market consideration
- Low power consumption
  - Portable device consideration
  - Short Range
- Unlicensed Used
  - ISM band used
- Robust operation
  - Fast frequency hopping
  - Short packet length
- Multiple links
- Mixed voice and data

ISM Unlicensed Band

- 79 channels in 2.4GHz (in USA and most Europe)

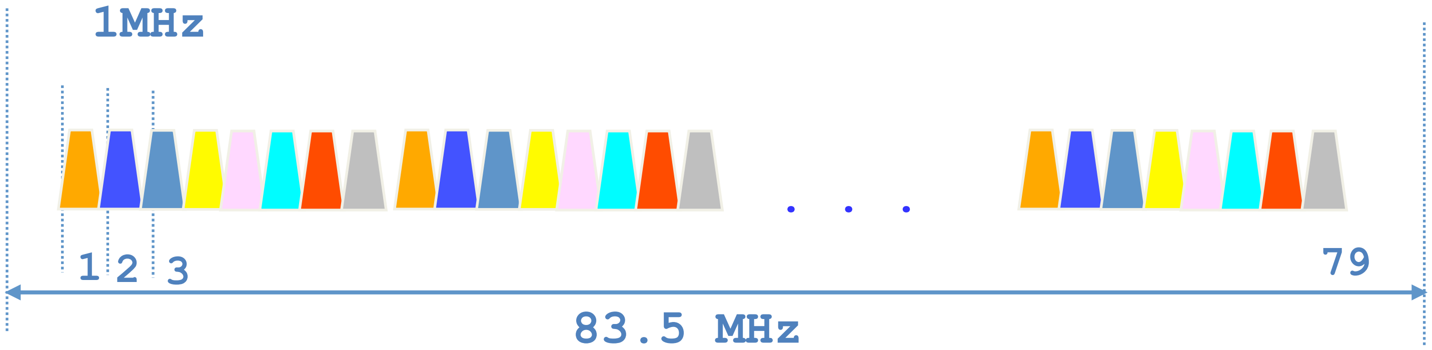


ISM unlicensed band

Frequency Range

- **2.4GHz ISM Frequency Range**

Country	**Frequency Range**	**RF Channels**	
Europe* & USA	2400 – 2483.5 MHz	f=2402 + k MHz	k=0,…,78
Japan	2471 – 2497 MHz	f=2473 + k MHz	k=0,…,22
Spain	2445 – 2475 MHz	f=2449 + k MHz	k=0,…,22
France	2446.5 – 2483.5 MHz	f=2454 + k MHz	k=0,…,22



Bluetooth Specifications

- 2.4 GHz ISM Unlicensed band
- Microwave ovens also use this band
- Frequency Hopping Spread Spectrum
  - Avoid interference
  - 23/79 channels
  - 1 MHz per channel
  - 1 Mbps link rate (GFSK modulation)
  - Fast frequency hopping and short data packets avoids interference
    - Nominally hops at 1600 times a second (vs. 2.5 hops/sec in IEEE 802.11)
    - 625us per hop (366us for data only)
    - 3200 times a second during inquiry and paging modes
- Multiple uncoordinated networks may exist and cause interference
  - CVSD (Continuous Variable Slope Delta Modulation) voice coding (FEC) enables operation at high bit error rates

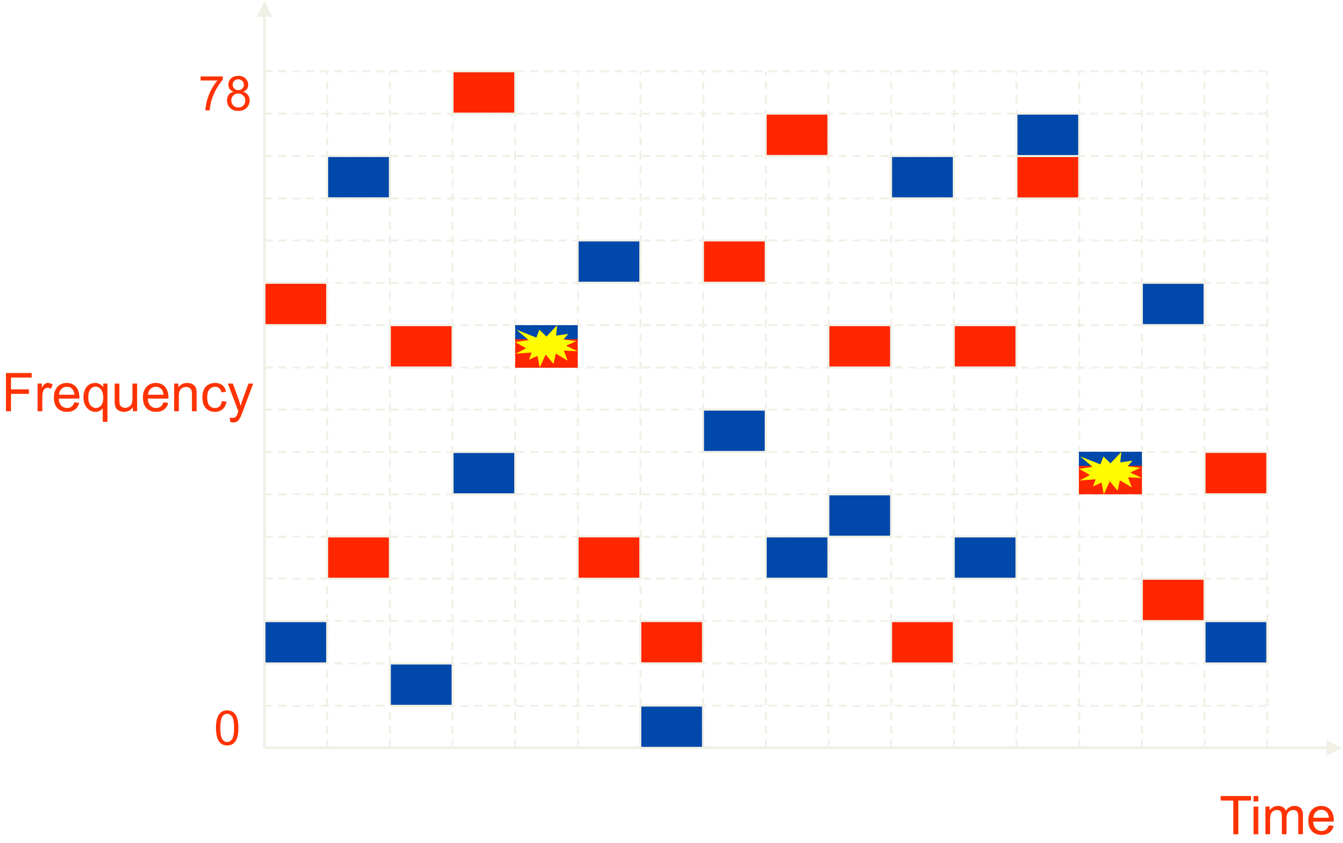
Transmit Power

- Transmit power and range
  - 0 dbm (up to 20dbm with power control)
  - 10-100 m

Power Class	Max Output	Min Output	Power Control
1	100mW (20dBm)	1mW (0dB)	-4db/time Max twice
2	2.5mW (4dBm)	0.25mW (-6dBm)	Optional
3	1mW (0dBm)	N/A	Optional

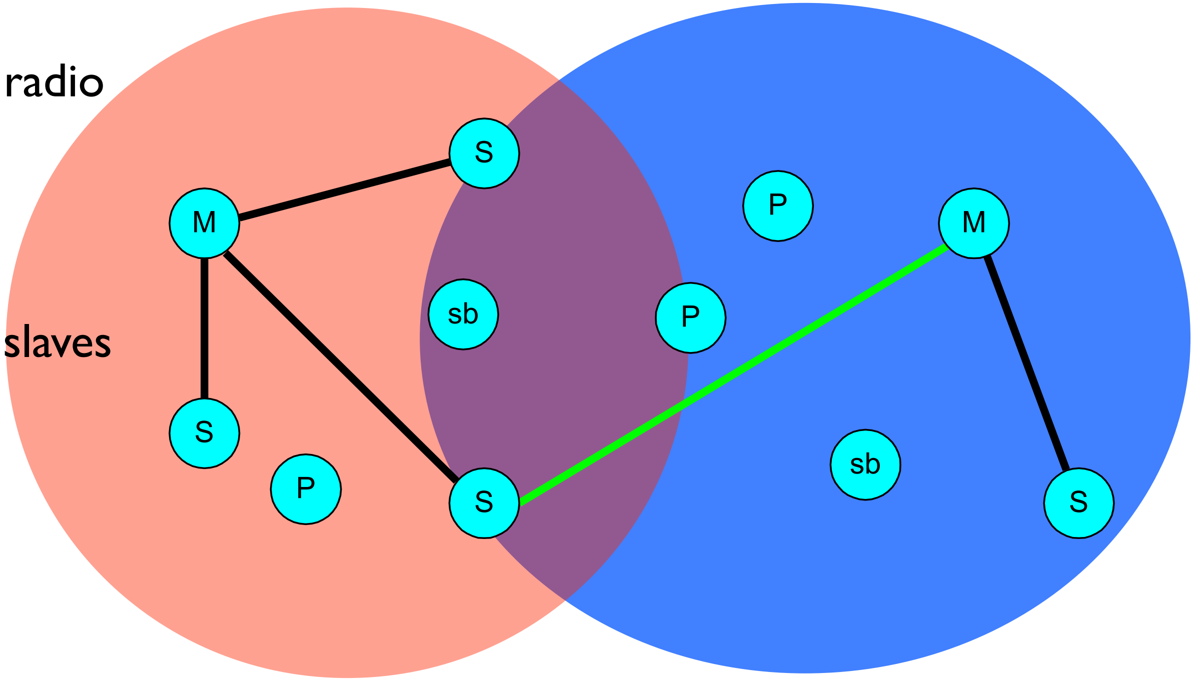
- **Power 1mW (class 3)**
  - **3% power of cellular phone**
  - **10meters of transmission distance or 100m by PA**
- **Power 100mW(class 1)**
  - **100 meters of transmission distance**

Frequency Hopping

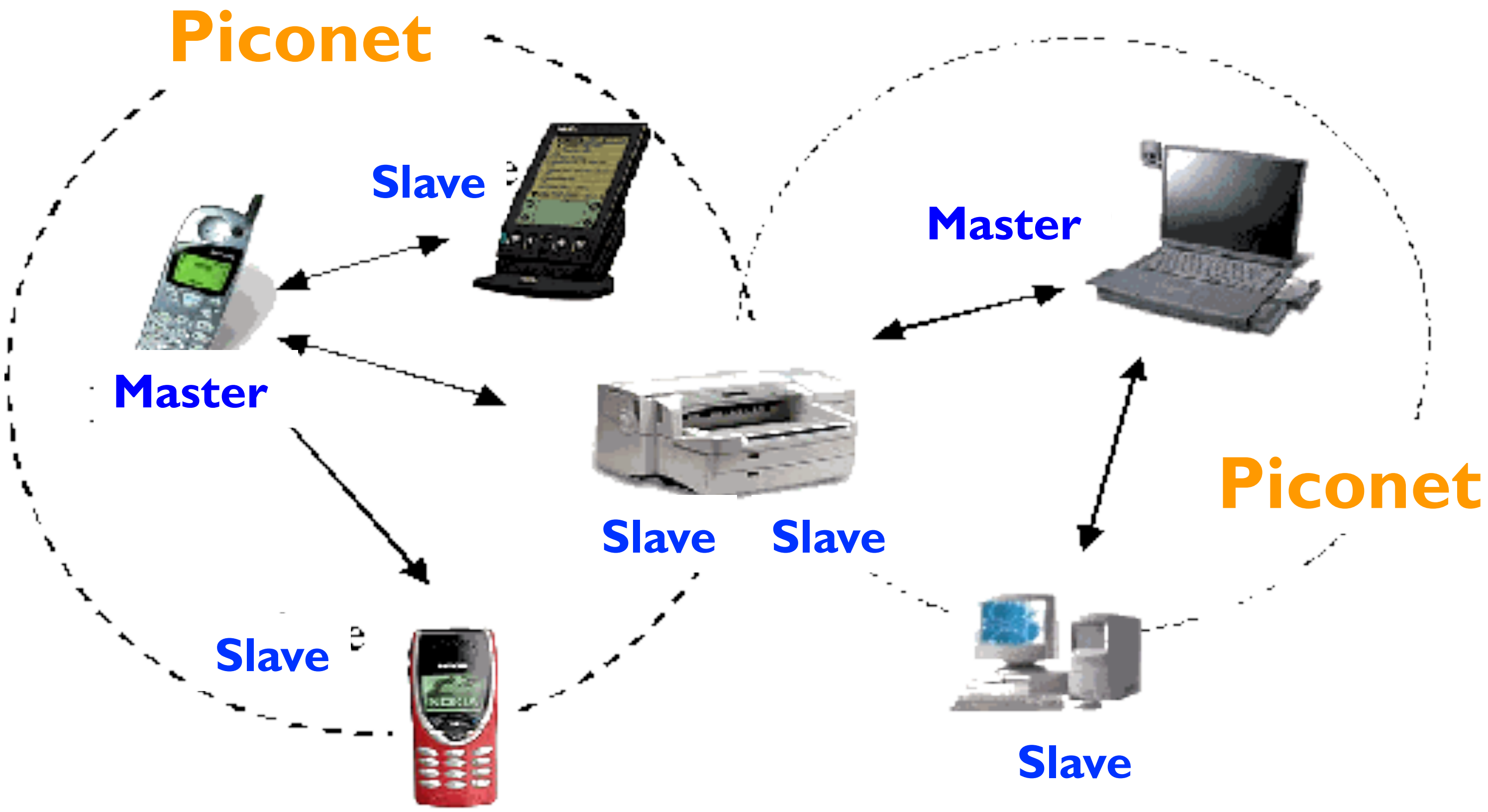


Bluetooth Architecture

- **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 Mbps)
    - Unique hopping pattern/ID
- **Scatternet**
  - High capacity system
    - Minimal impact with up to 10 piconets within range
  - Radios can share piconets!

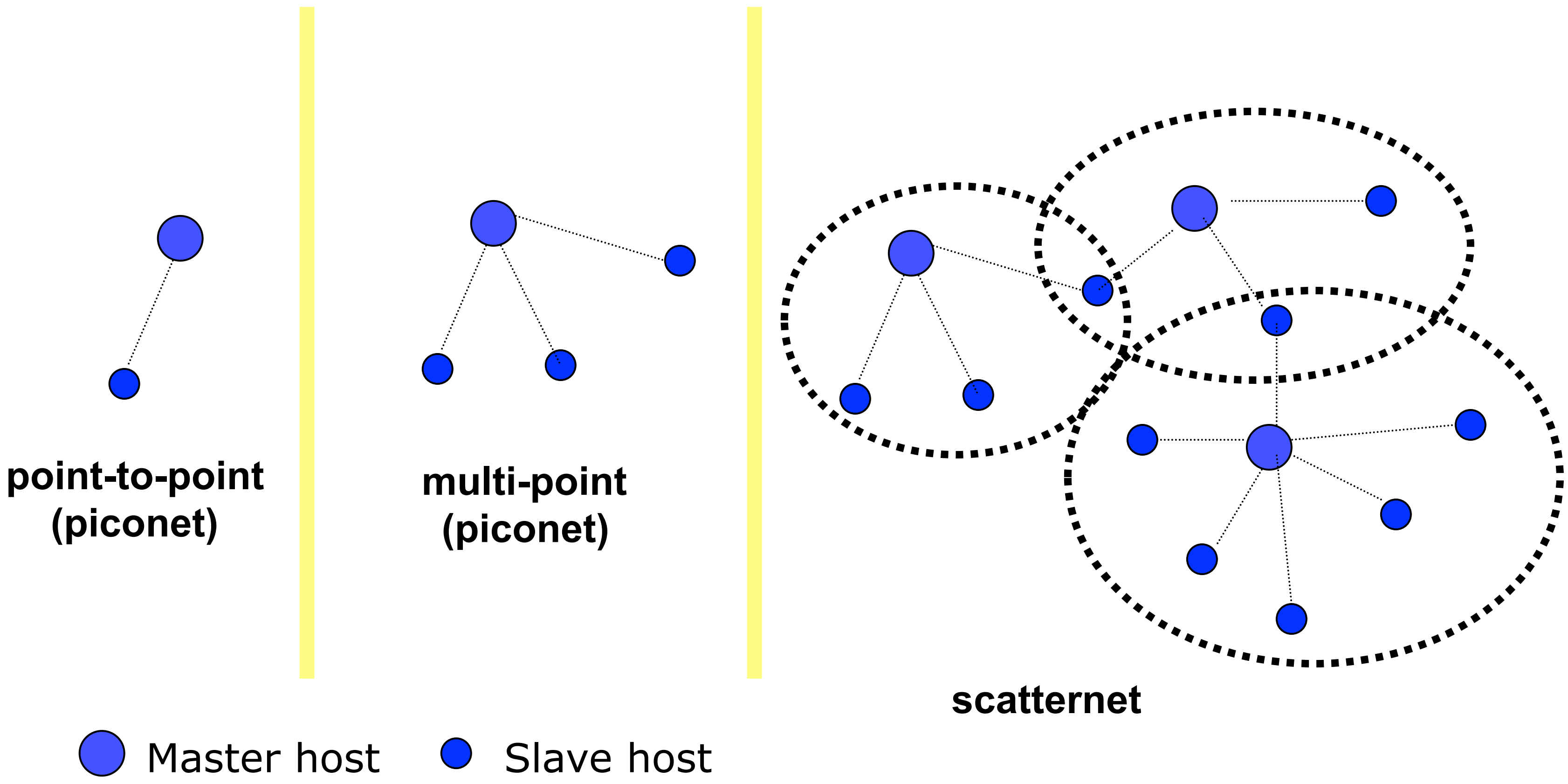


Scatternet



Scatternet contains two piconets

Piconet vs. Scatternet



point-to-point
(piconet)

multi-point
(piconet)

scatternet

● Master host ● Slave host

Device Addressing (1/2)

- Every Bluetooth device has **unique 48-bit** Bluetooth Device Address (BD_ADDR)
- The **BD_ADDR** is used to control the system functions :
  - Hopping sequence
  - Channel access code
  - Encryption key
- The **BD_ADDR** contains 3 parts:
  - 24-bit Lower Address Part (LAP)
    - Used to identify unique BT device (reduce overhead)
  - 8-bit Upper Address Part (UAP)
    - Used to determine the hopping sequence
  - 16-bit Non-significant Address Part (NAP)

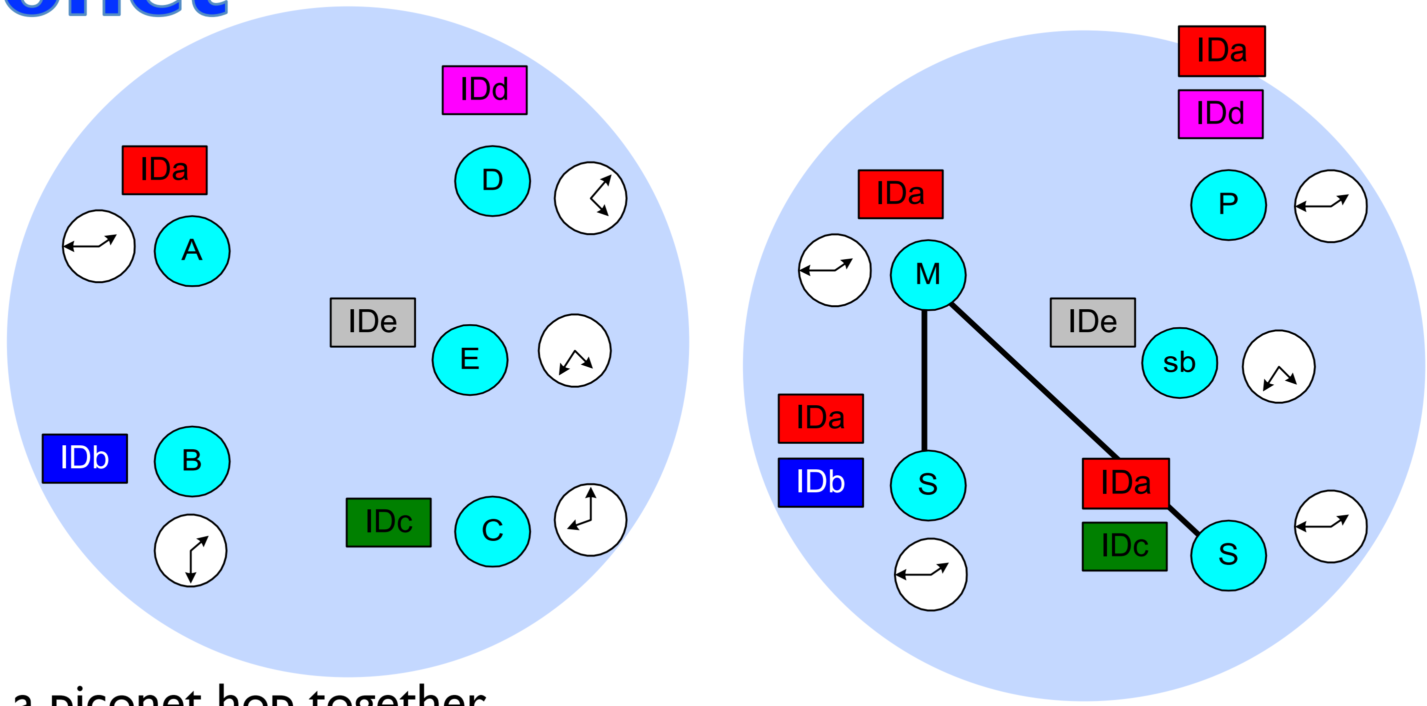
	16	8	24	bits
BD_ADDR	NAP	UAP	LAP	

Device Addressing (2/2)

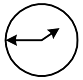
- **AM_ADDR (Active Member Address)**
  - Each slave is assigned a 3-bit address
  - 7 slaves in a piconet is available
  - 000 : for broadcasting packets (i.e., master address)
    - An exception is FHS (Frequency Hopping Synchronization) packet which may use "000" address but is not a broadcast message
  - Slaves that are disconnected or parked give up their AM_ADDRs

- **PM_ADDR (Parked Member Address)**
  - Slaves that enter the park mode will obtain a 8-bit PM_ADDR
  - At most 256 slaves are in park mode in a piconet

The Piconet



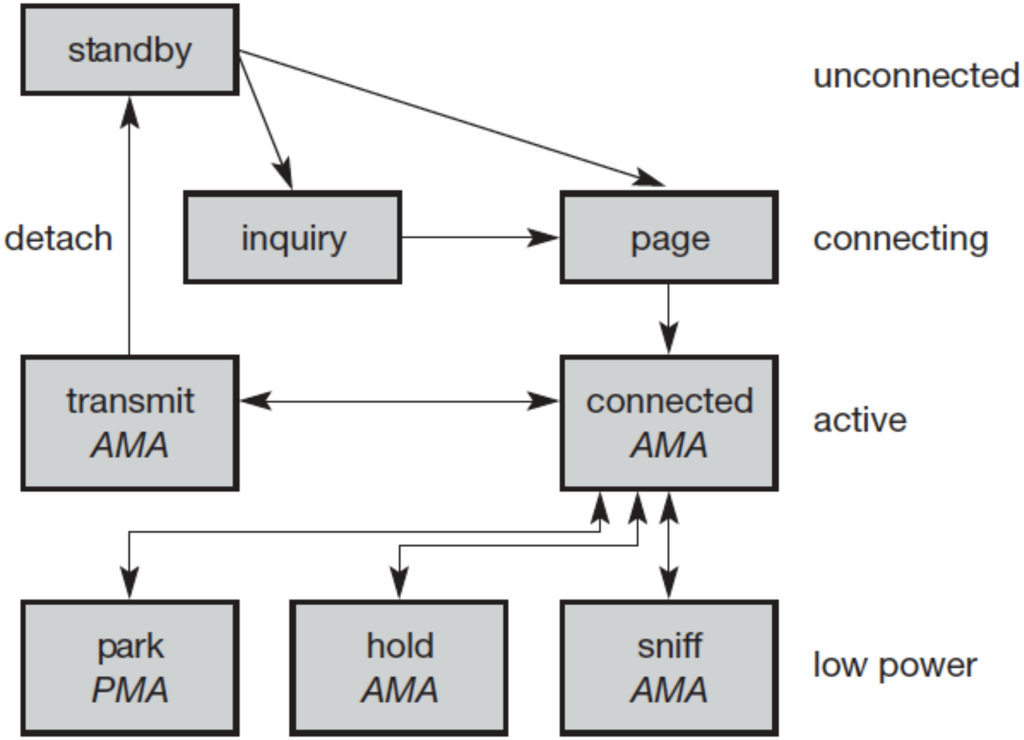
- All devices in a piconet hop together
  - In forming a piconet, master gives slaves its *clock* and *device ID* (BD_ADDR) via FHS packet
    - Hopping pattern determined by *device ID* (48-bit) IDa
    - Phase in hopping pattern determined by *Clock*



- Non-piconet devices are in standby sb
- Piconet Addressing
  - *Active Member Address* (AMA, 3-bits) M **or** S
  - *Parked Member Address* (PMA, 8-bits) P

Connection Procedure

- 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/Sniff/Hold
  - Low Power connected states



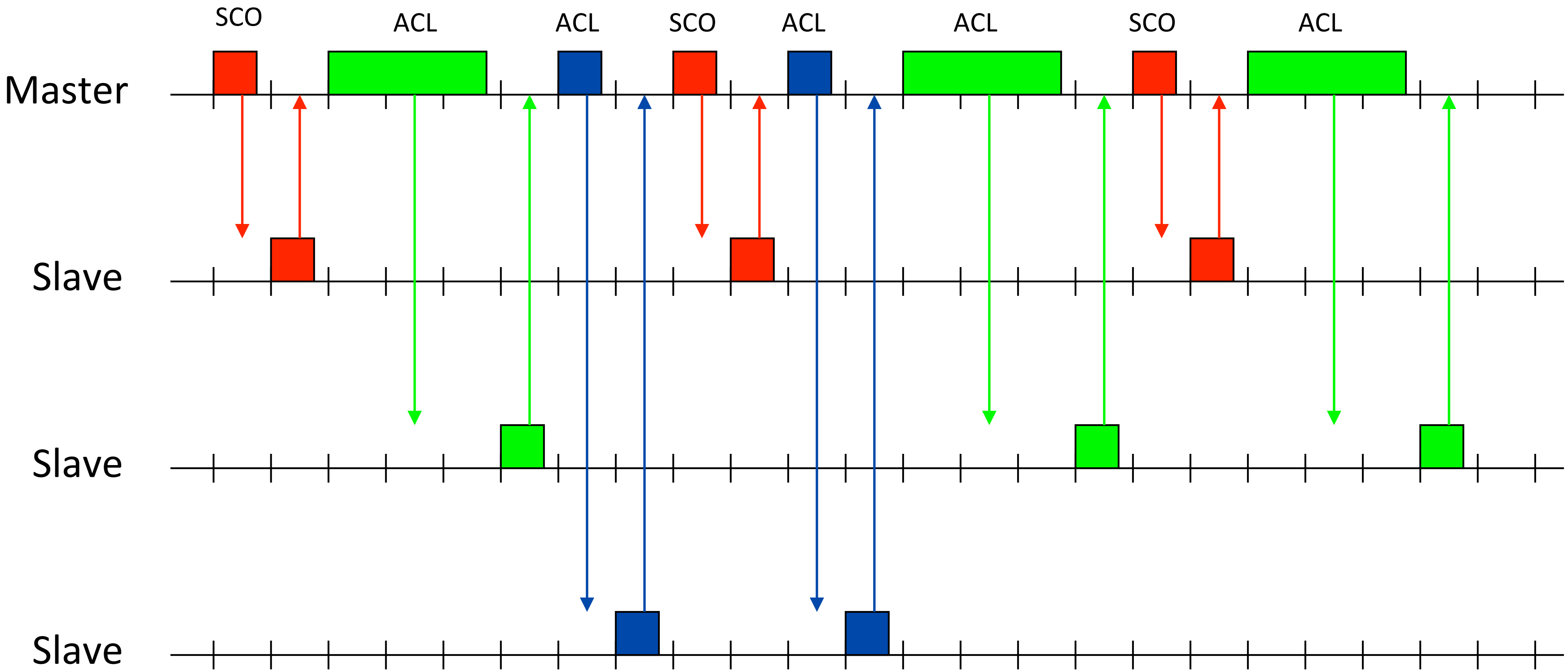
Sniff, Hold, and Park States

1. **Sniff:**
   the device listens to the piconet at a reduced rate. The device keeps its AMA
2. **Hold:**
   The device does not release its AMA but stops **ACL** transmission. A slave may still exchange **SCO** packets.
3. **Park:**
   The device releases its AMA and receives a parked member address (PMA).

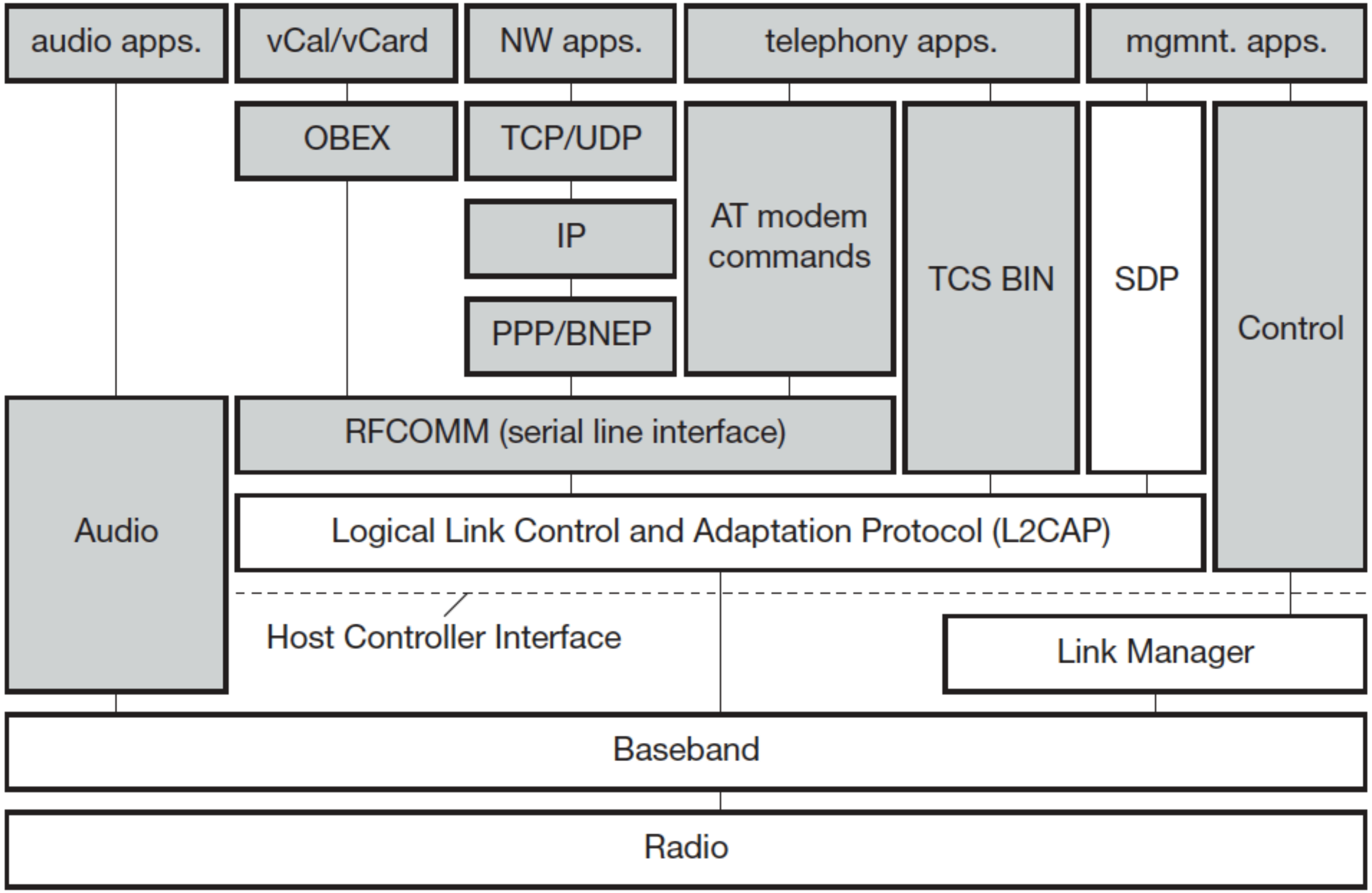
Bluetooth Link Types

- **Synchronous Connection Oriented (SCO)**
  - Circuit switched typically used for voice
  - Symmetric, synchronous service
  - Slot reservation at fixed intervals
  - Point-to-point
- **Asynchronous Connectionless Link (ACL)**
  - Packet switched
  - Symmetric or asymmetric, asynchronous service
  - Polling mechanism between master and slave(s)
  - Point-to-point and point-to-multipoint

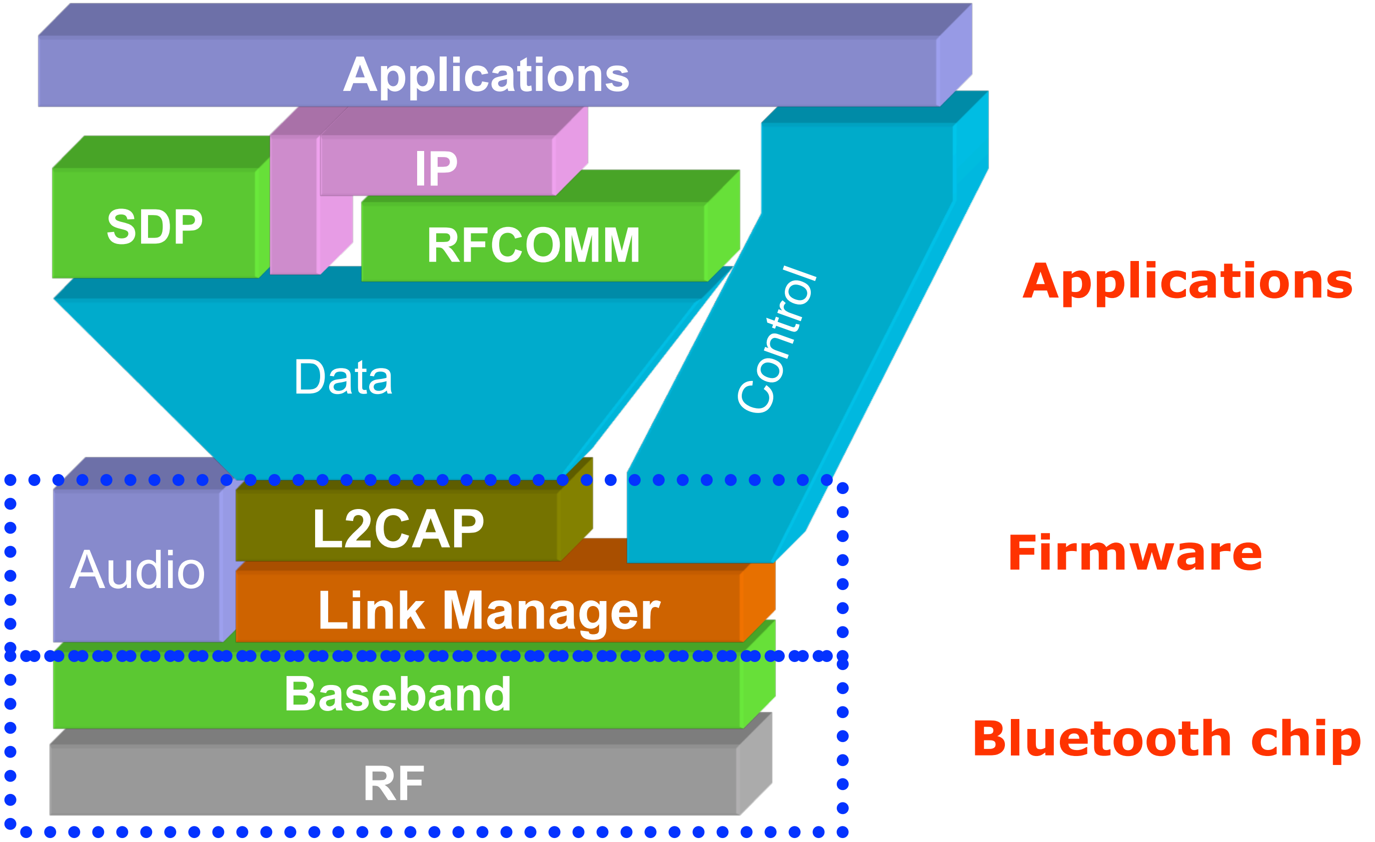
Voice and Data Transmission: An Example



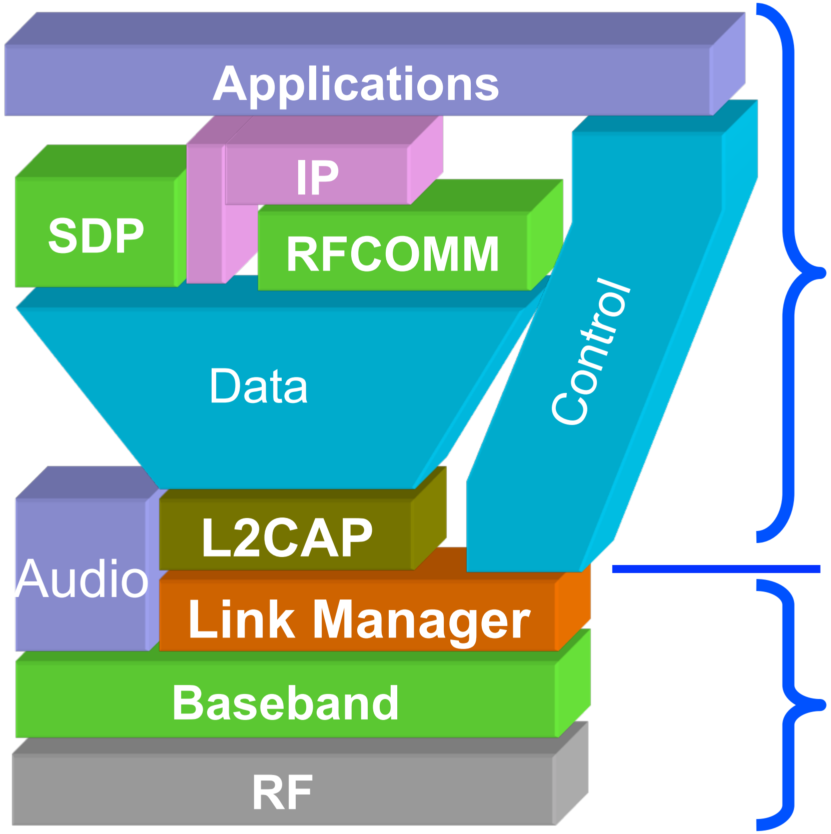
Bluetooth Protocol Stack



Bluetooth Protocol Stack



Bluetooth Certifications



Application Framework Certification

Service	Lower Interface Type	 Class	Certification Class
vCard	IrOBEX	BT.OBEX	BT.vCard
vCal	IrOBEX	BT.OBEX	BT.vCal
UDP	PPP	BT.PPP	BT.UDP
PPP	RFCOMM	BT.TS0710	BT.PPP
IrOBEX	RFCOMM	BT.TS0710	BT.OBEX
WAP	TCP/IP	BT.TCP/IP	BT.WAP
Still Images	HID	BT.HID	BT.SImg
Audio Ctrl	L^{2}CAP	BT.L^{2}CAP-A	BT.AudioCtrl
RFCOMM	L^{2}CAP	BT.L^{2}CAP-D	BT.TS0710
TCP/IP	L^{2}CAP	BT.L^{2}CAP-D	BT.TCP/IP
HID	L^{2}CAP	BT.L^{2}CAP-D	BT.HID

HCI: Host Controller Interface

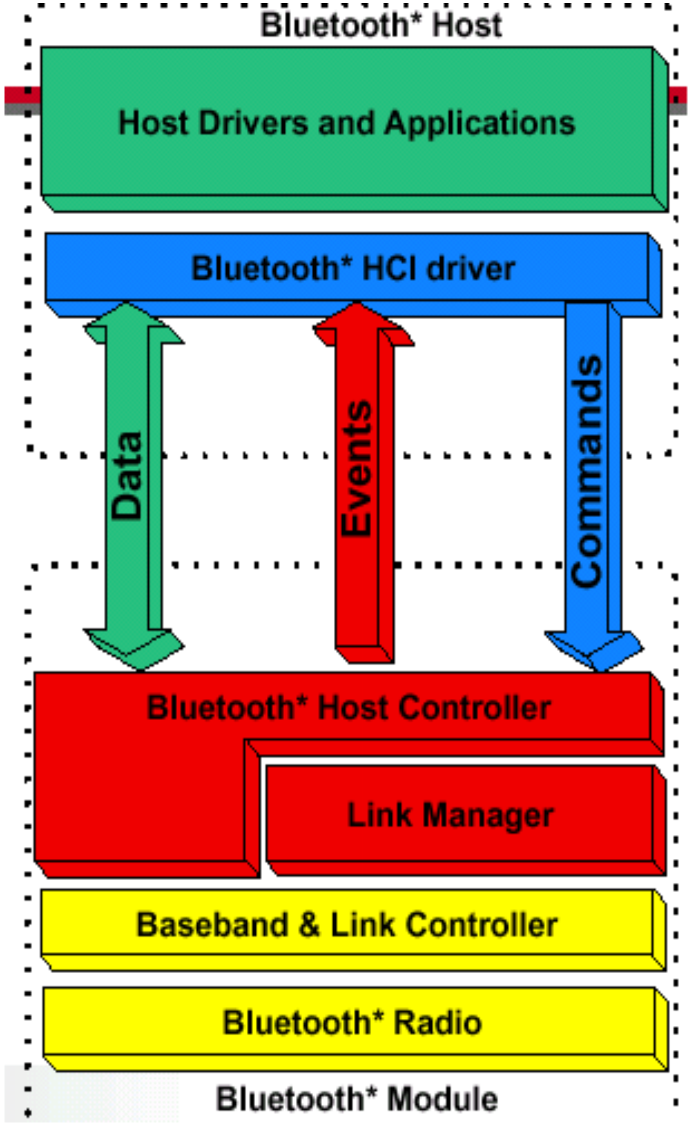
Service	Lower Interface Type	 Class Audio	 Data	Certification Class Audio	 Data
L^{2}CAP	LM	BT.LM-A	BT.LM-D	BT.L^{2}CAP-A	BT.L^{2}CAP-D
LM	BB	BT.BB-A	BT.BB-D	BT.LM-A	BT.LM-D
BB	RF	BT.RF	BT.RF	BT.BB-A	BT.BB-D
RF	Air	-	-	BT.RF	BT.RF

A unit that supports both audio and data gets the certification class A and D.
Example: BT.BB-A,D

Basic Layer Certification

Host Control Interface (HCI)

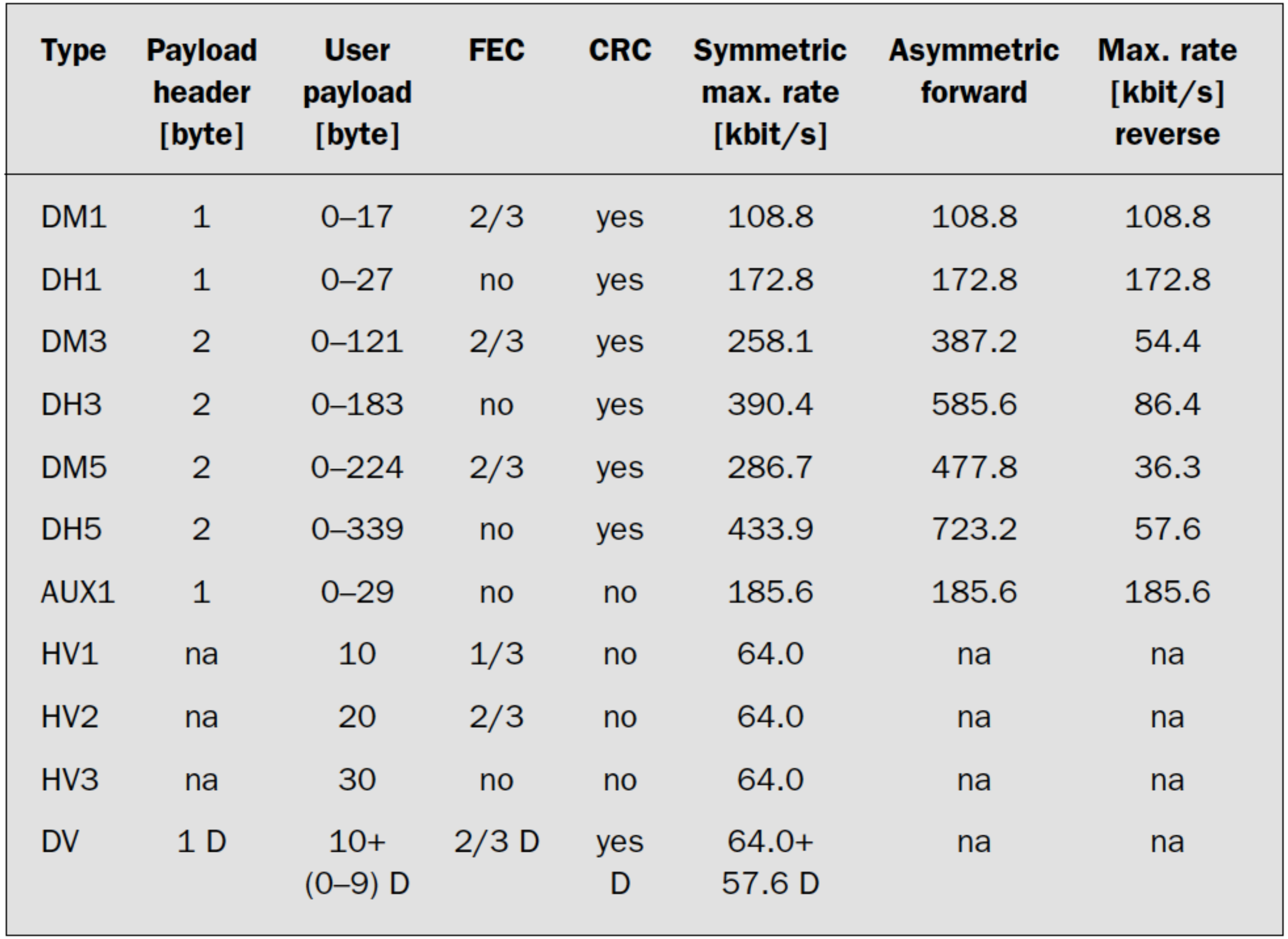
- **All HCI transactions are framed in packets:**
  - Commands
  - Event
  - Data (ACL)
  - Data (SCO)



Baseband Data Rules

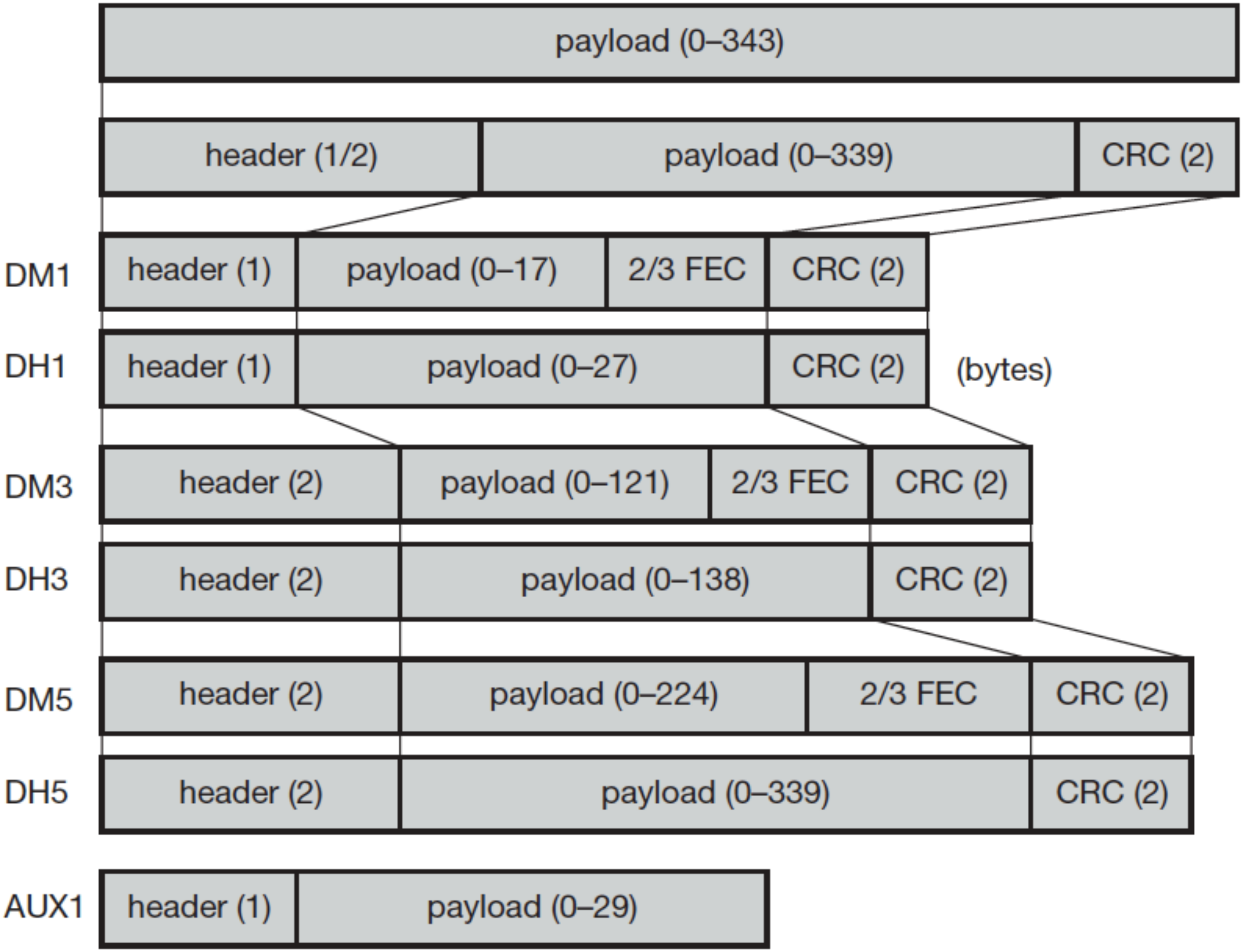
ACL

SCO



Type	Payload header [byte]	User payload [byte]	FEC	CRC	Symmetric max. rate [kbit/s]	Asymmetric forward	Max. rate [kbit/s] reverse
DM1	1	0–17	2/3	yes	108.8	108.8	108.8
DH1	1	0–27	no	yes	172.8	172.8	172.8
DM3	2	0–121	2/3	yes	258.1	387.2	54.4
DH3	2	0–183	no	yes	390.4	585.6	86.4
DM5	2	0–224	2/3	yes	286.7	477.8	36.3
DH5	2	0–339	no	yes	433.9	723.2	57.6
AUX1	1	0–29	no	no	185.6	185.6	185.6
HV1	na	10	1/3	no	64.0	na	na
HV2	na	20	2/3	no	64.0	na	na
HV3	na	30	no	no	64.0	na	na
DV	1 D	10+ (0–9) D	2/3 D	yes D	64.0+ 57.6 D	na	na

ACL Payload Types



payload (0–343)

header (1/2) | payload (0–339) | CRC (2)

DM1 header (1) | payload (0–17) | 2/3 FEC | CRC (2)

DH1 header (1) | payload (0–27) | CRC (2)

(bytes)

DM3 header (2) | payload (0–121) | 2/3 FEC | CRC (2)

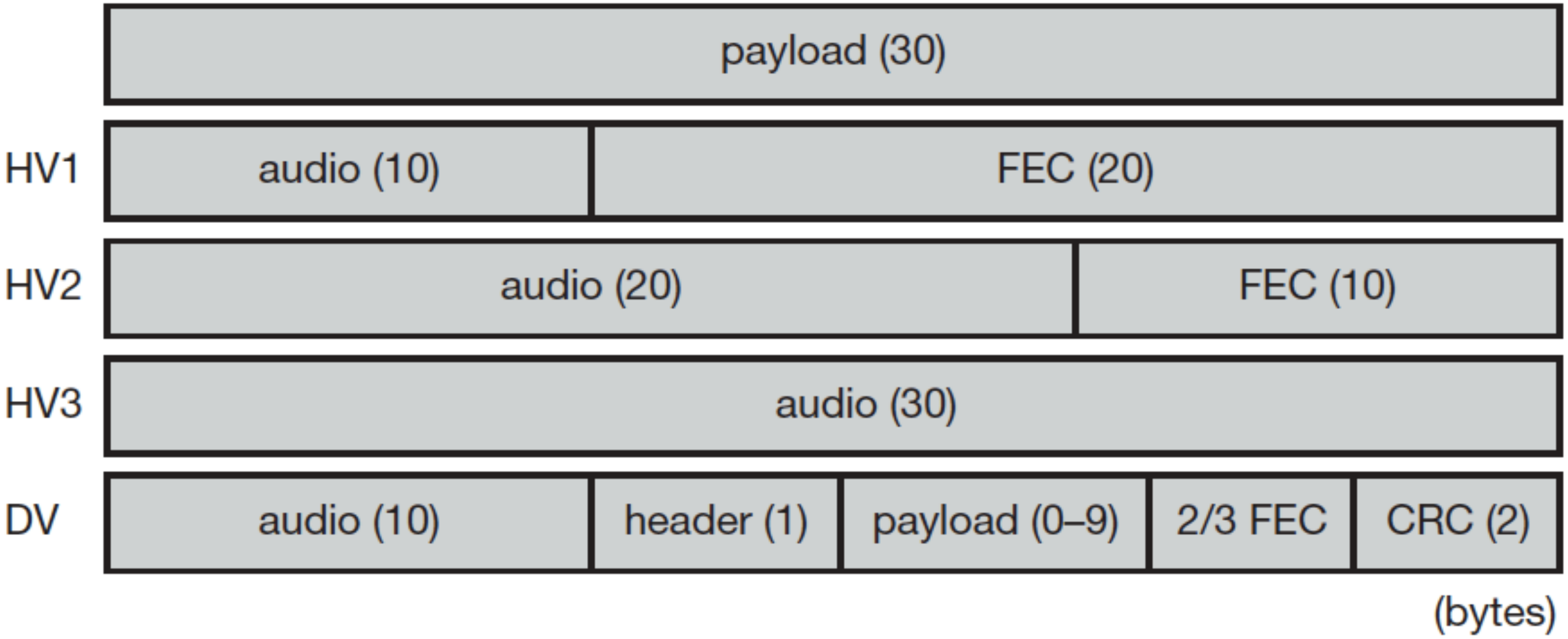
DH3 header (2) | payload (0–138) | CRC (2)

DM5 header (2) | payload (0–224) | 2/3 FEC | CRC (2)

DH5 header (2) | payload (0–339) | CRC (2)

AUX1 header (1) | payload (0–29)

SCO Payload Types



payload (30)

HV1 audio (10) FEC (20)

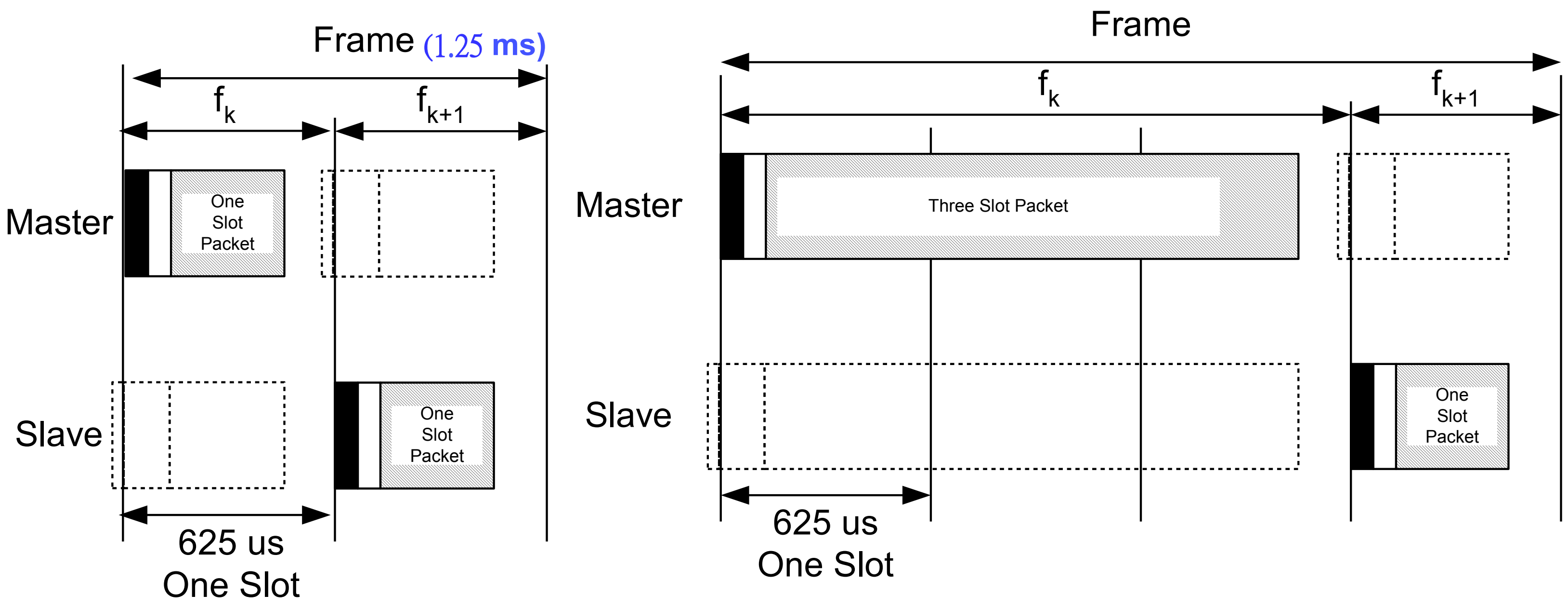
HV2 audio (20) FEC (10)

HV3 audio (30)

DV audio (10) header (1) payload (0–9) 2/3 FEC CRC (2)

(bytes)

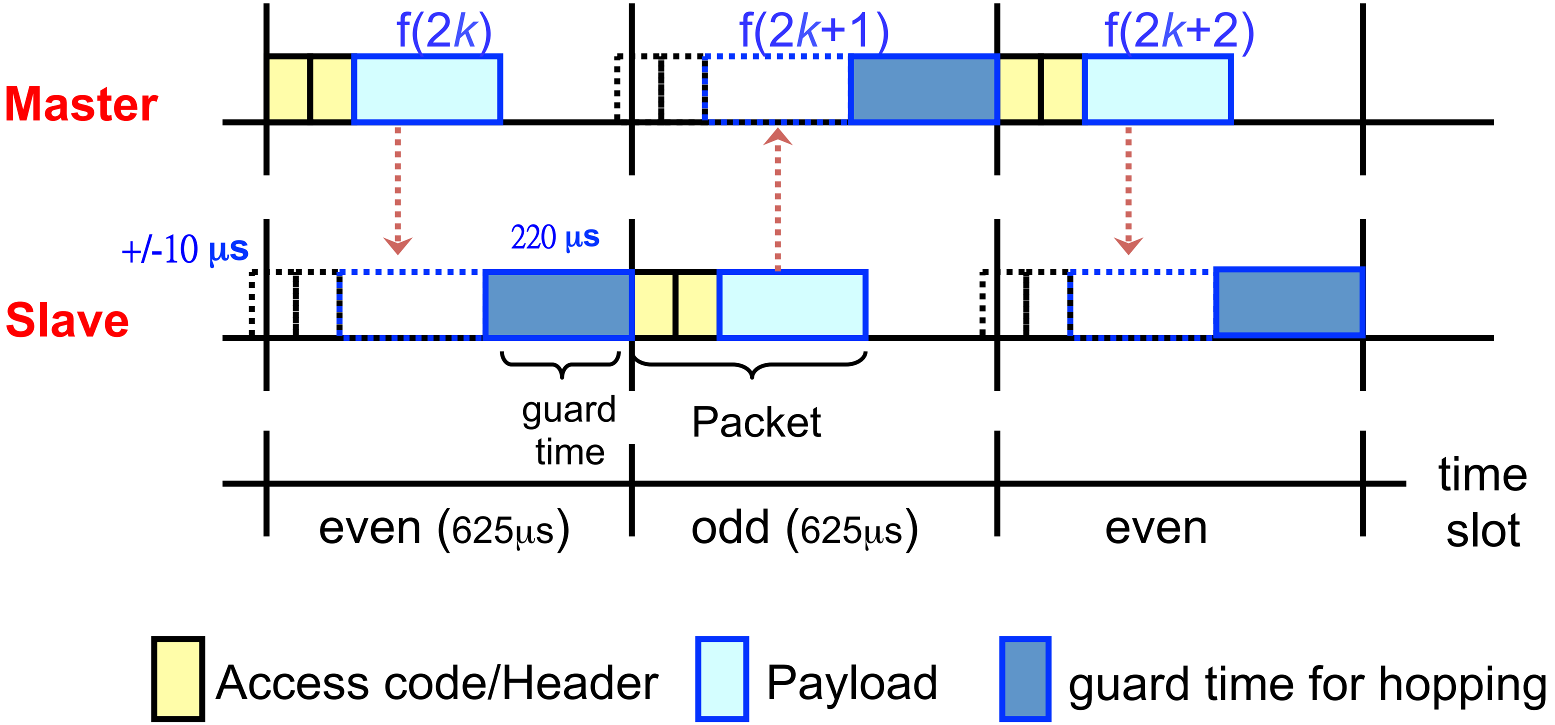
Basic Baseband Protocol



- Spread spectrum frequency hopping radio
  - **Hops every packet**
    - Packets are 1, 3 or 5 slots long
  - **Frame consists of two packets**
    - Transmit followed by receive
  - **Nominally hops at 1600 times a second (1 slot packets)**

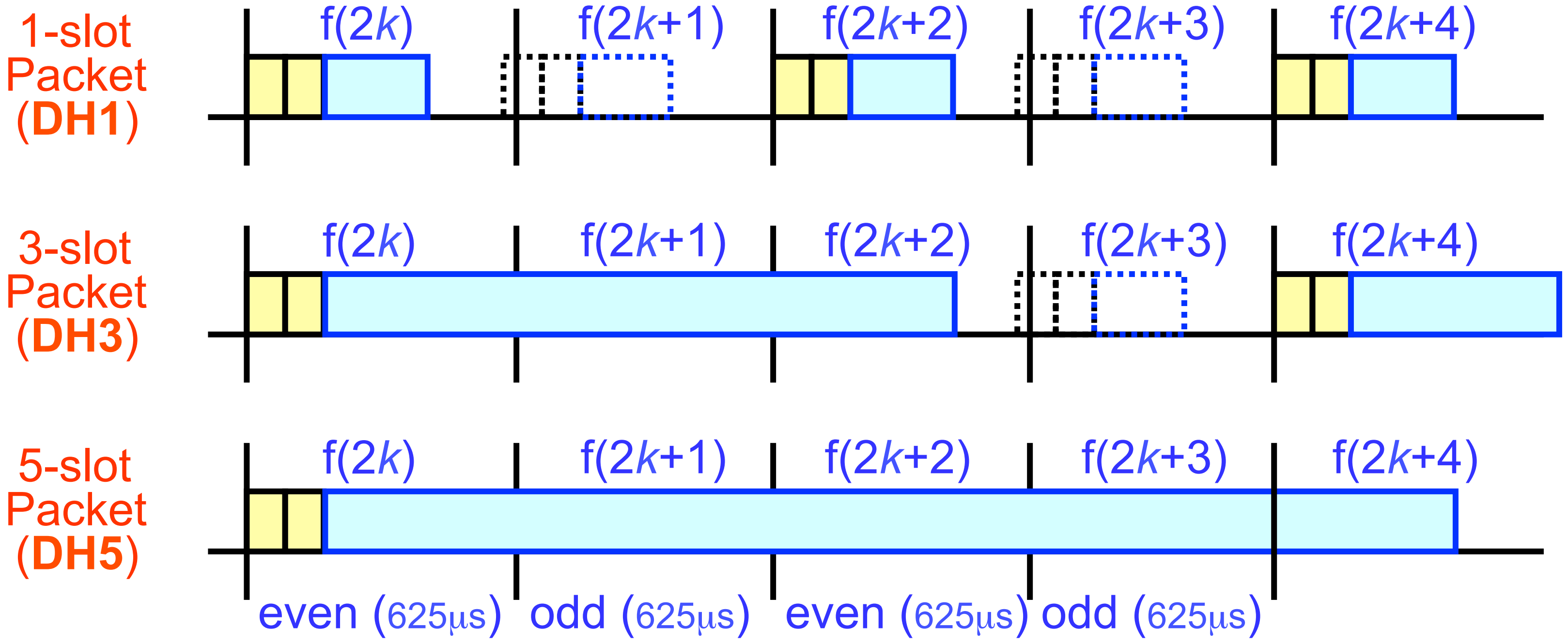
Time Division Duplex (TDD)

- Master : **even** numbered slots
- Slave : **odd** numbered slots
- The Slot Number ranges from **0- 2^{27}-1**.

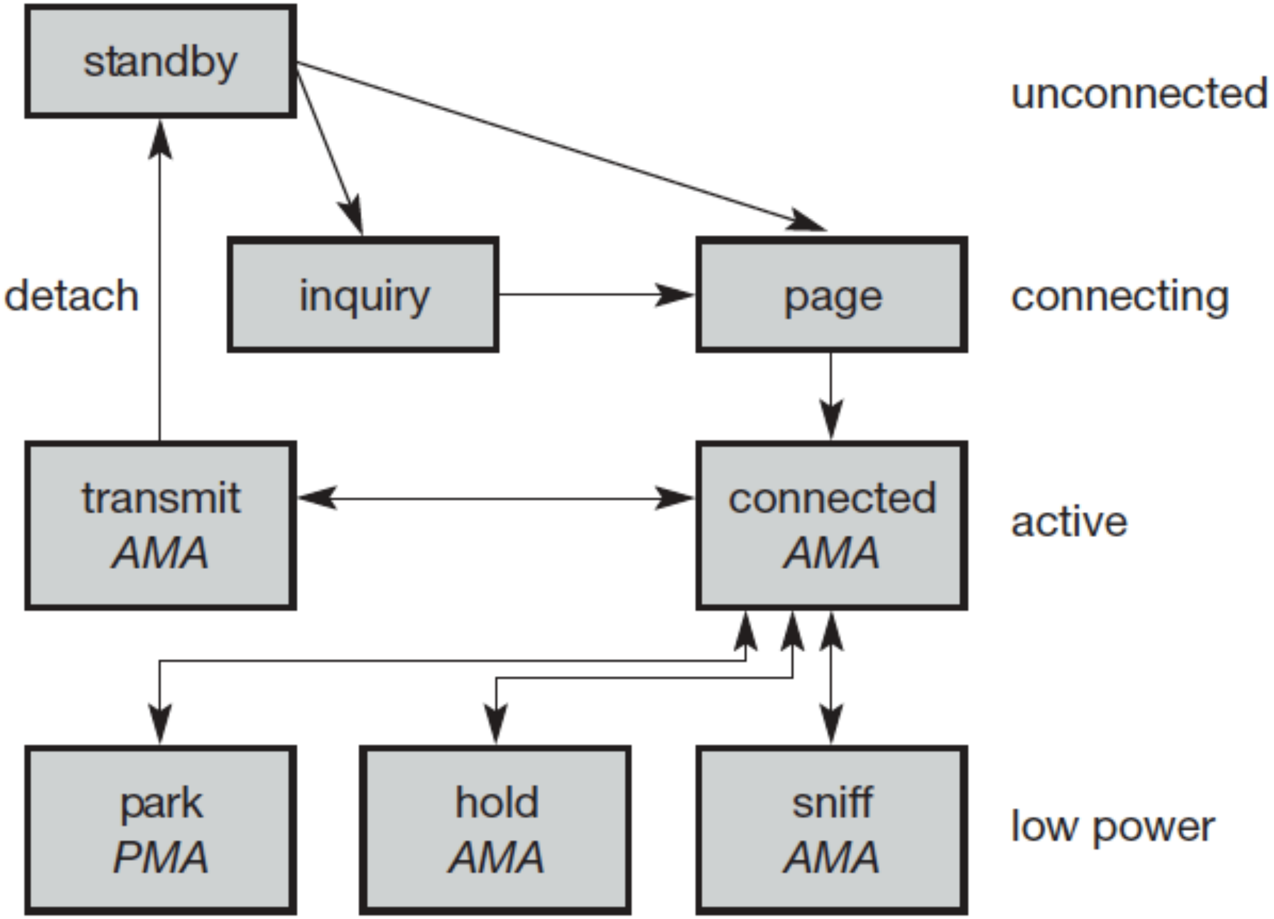


Multi-slot Packets

- Different packet overhead will result in different throughput
  - **DH1 : 172.8Kbps** in Sym. and Asy. modes
  - **DH3 : 390.4Kbps** in Sym. mode; 387.2 and 54.4Kbps in Asy. Mode
  - **DH5 : 433.9Kbps** in Sym. mode; 721 and 57.6Kbps in Ays.
    - DH : without FEC



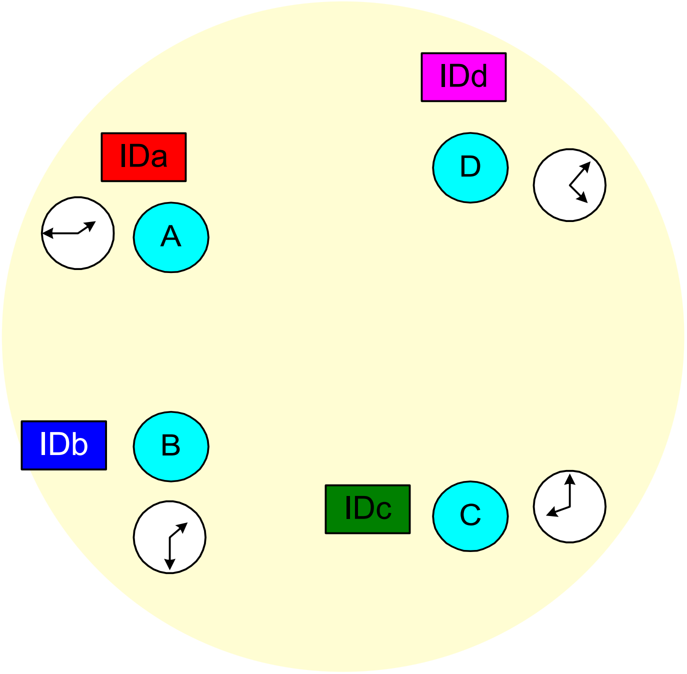
Bluetooth Baseband States



Page and Inquire Scans

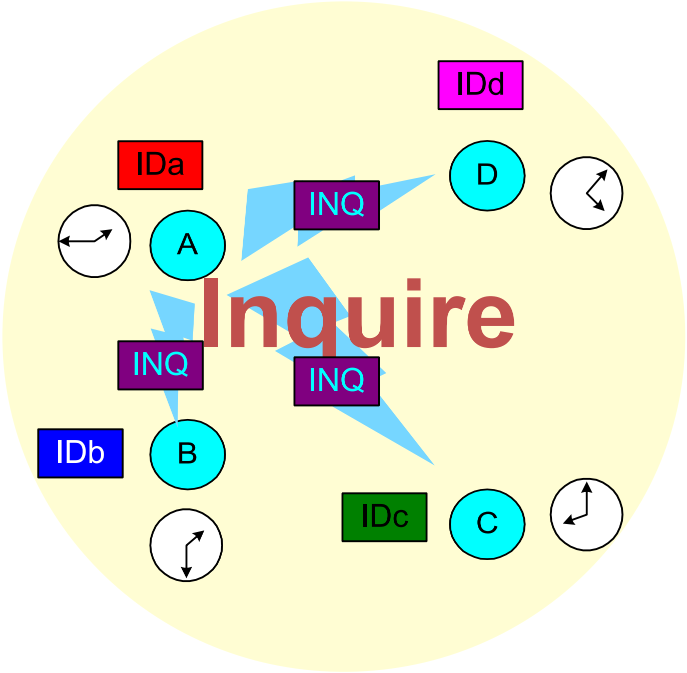
- **Inquiry Scan:**
  - 32 channels (of 79 channels) are assigned for inquiry procedure
  - 32 channels are divided as 2 trains (Trains A and B), each one contains 16 channels.
- **Page Scan:**
  - 32 channels (of 79 channels) are assigned for page procedure
  - 32 channels are divided as 2 trains (Trains A and B), each one contains 16 adjacent channels.
  - Train A : f(k-8), f(k-7), … f(k), f(k+1), … , f(k+7)
  - Train B : f(k-16), f(k-15), … f(k-9), f(k+8), … , f(k+15)
- **Broadcast ID packet**, with specified *General Inquiry Access Code* (GIAC) or *Dedicated Inquiry Access Code* (DIAC)

Inquiring for Radios



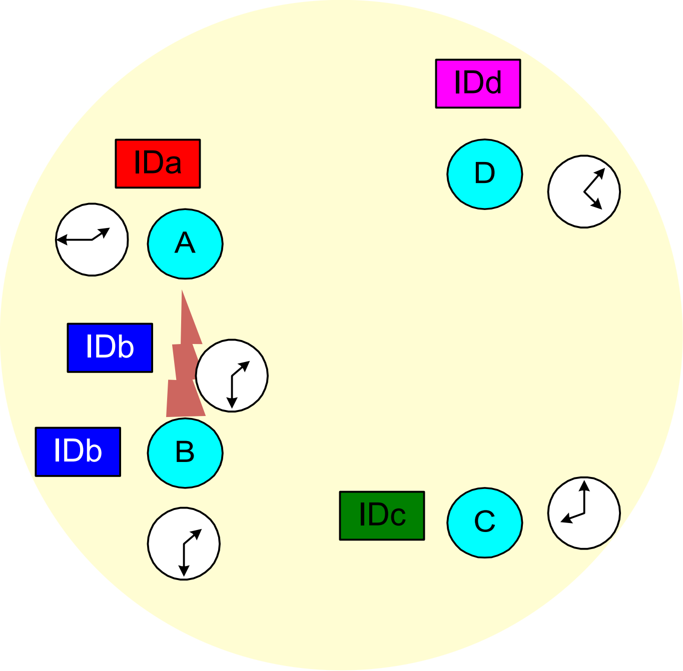
- Radio wants to find other radios in the area

Inquiring for Radios



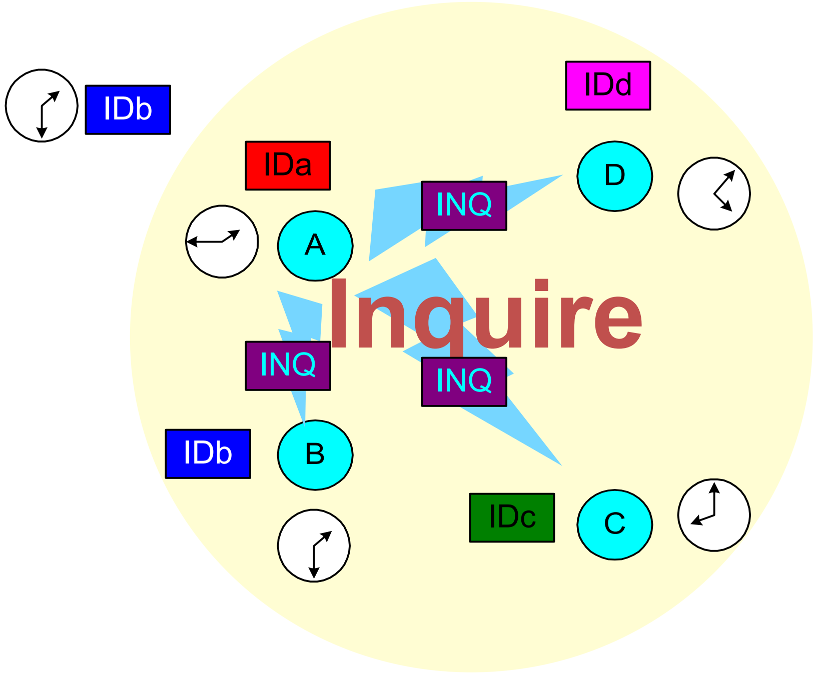
- Radio Wants to find other radios in the area
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing an Inquire Scan

Inquiring for Radios



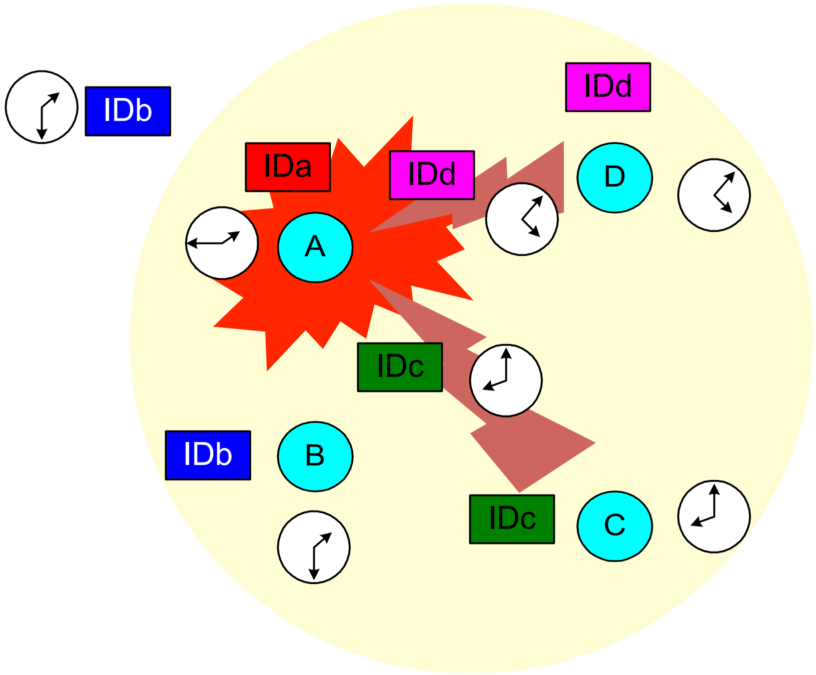
- Radio Wants to find other radios in the area
  - – Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing a Inquire Scan
  - – Radio B recognizes Inquire and responds with an FHS (Frequency Hopping Synchronization) packet
    - Has slave's *Device ID* and *Clock*

Inquiring for Radios



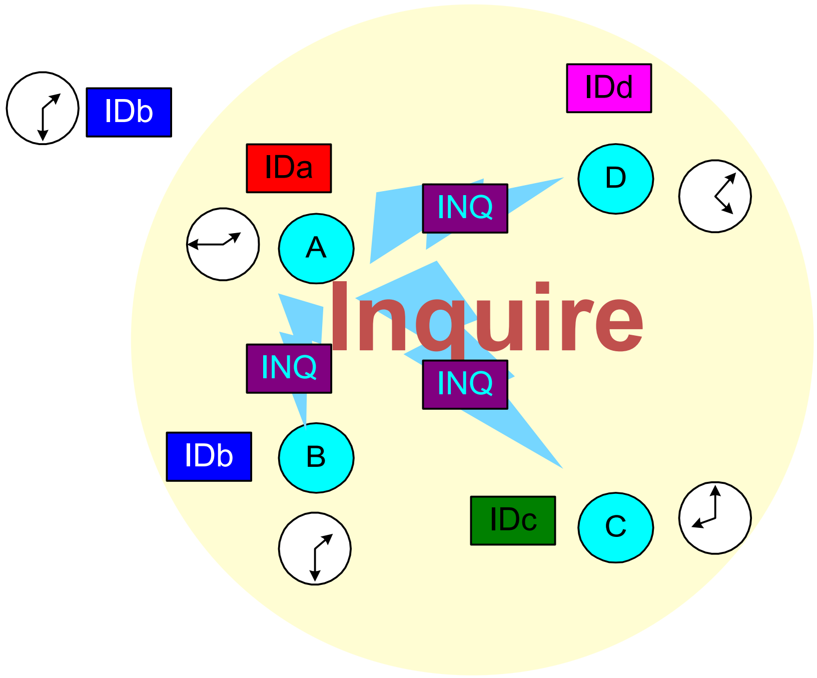
- Radio Wants to find other radios in the area
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing a Inquire Scan
  - Radio B recognizes Inquire and responds with an FHS packet
    - Has slave's *Device ID* and *Clock*

Inquiring for Radios



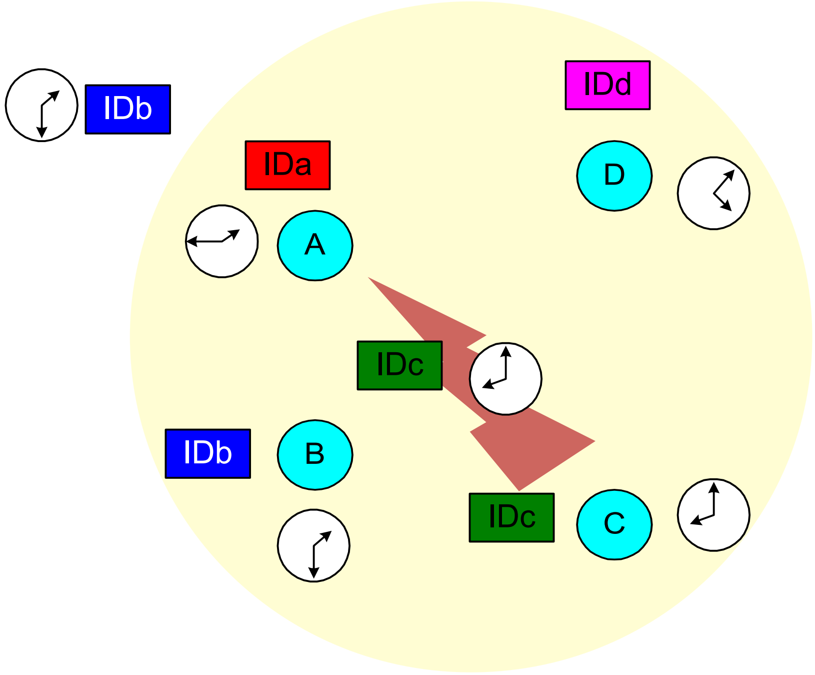
- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
  - Radios C and D respond with FHS packets
    - As radios C & D respond simultaneously packets are corrupted and Radio A won’t respond
    - Each radio **waits a random number of slots** and listens

Inquiring for Radios



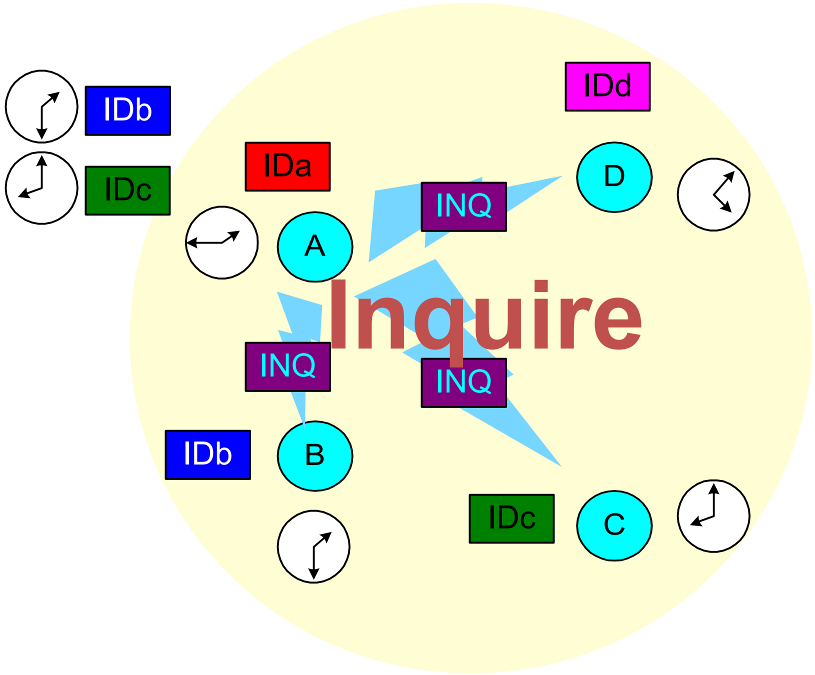
- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)

Inquiring for Radios



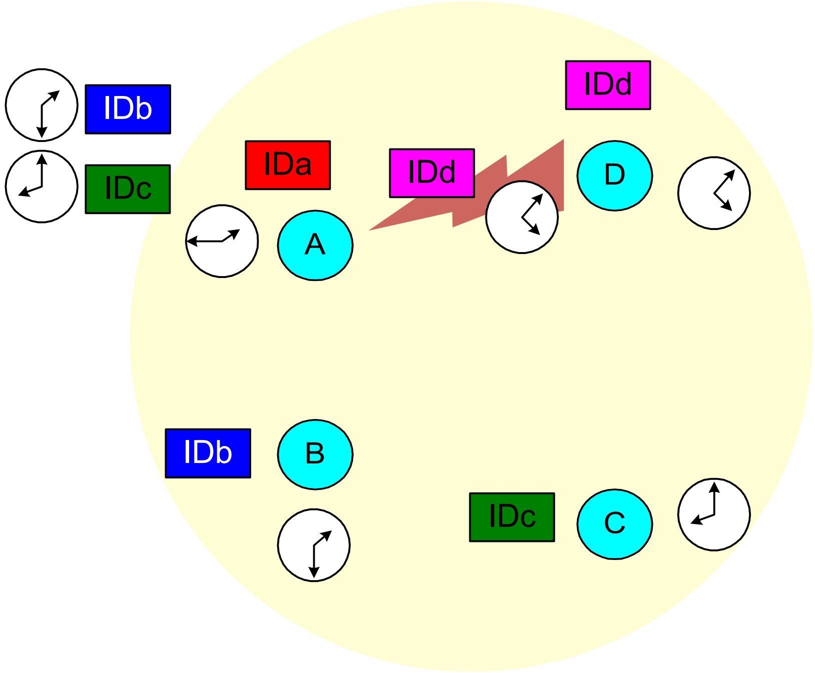
- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
  - Radios C respond with FHS packets

Inquiring for Radios



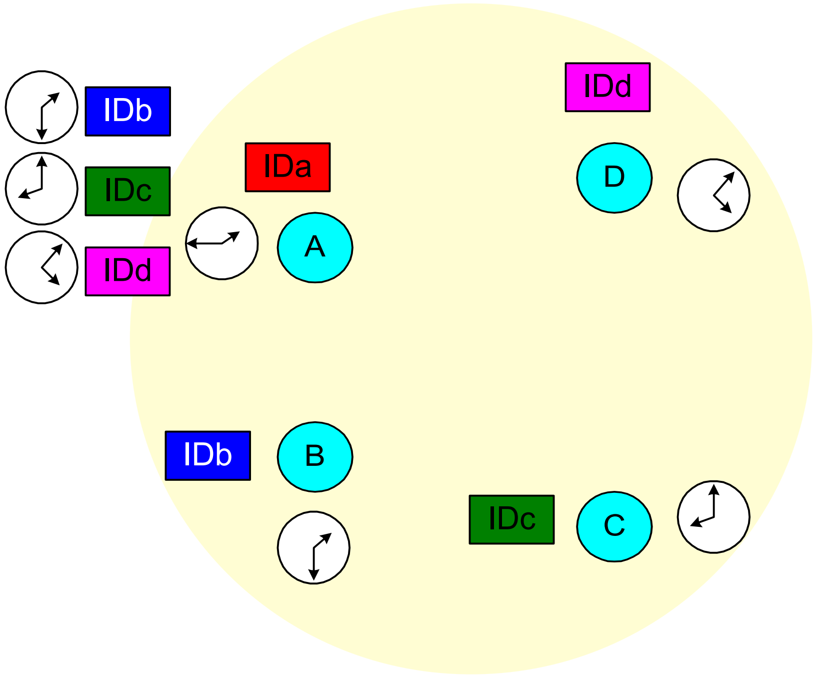
- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)

Inquiring for Radios



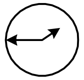
- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
  - Radios D respond with FHS packets

Inquiring for Radios

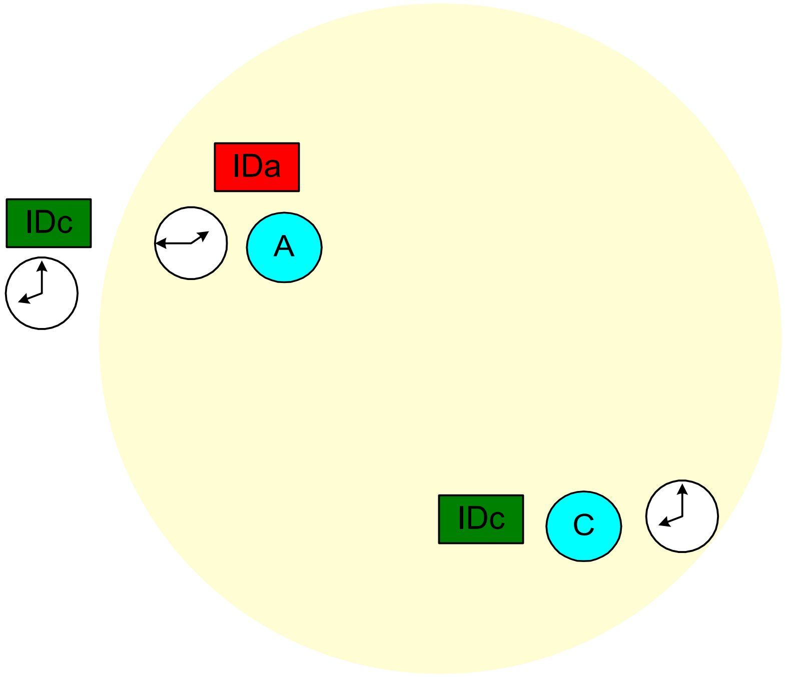


- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
  - Radios D respond with FHS packets
  - Radio A now has information of all radios within range

Inquire Summary

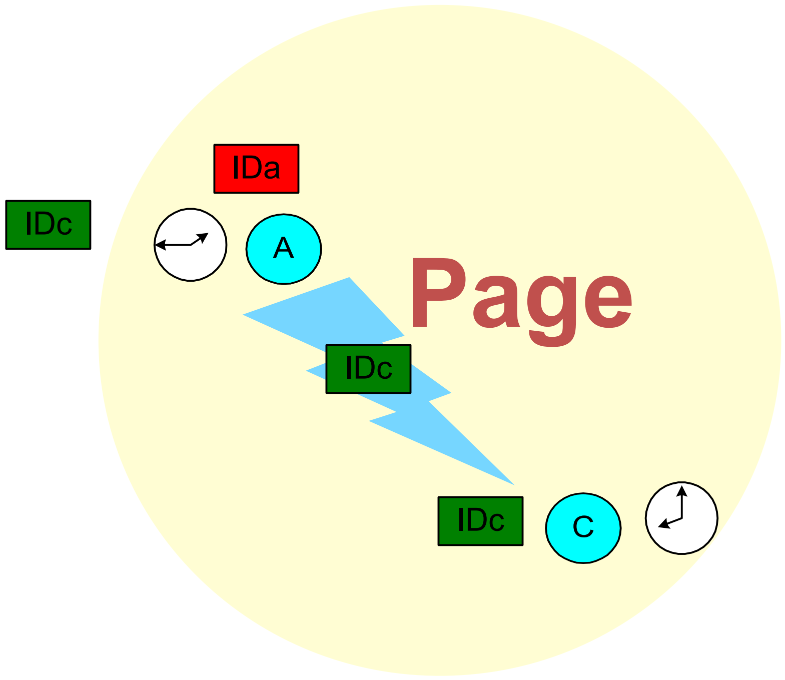
- Inquiring radio Issues inquiry packet with Inquire ID (**GIAC** or **DIAC** access code)
- Any radio doing an Inquire scan will respond with an **FHS** packet
  - FHS packet gives Inquiring radio information to page
    - *Device ID* IDa
    - *Clock* 
  - If there is a collision then radios wait a random number of slots before responding to the page inquire
- After process is done, Inquiring radio has *Device IDs* and *Clocks* of all radios in range
- Slave listens one of 16 channels for sufficient time (e.g., 18 slots=11.25ms)

Master Paging a Slave



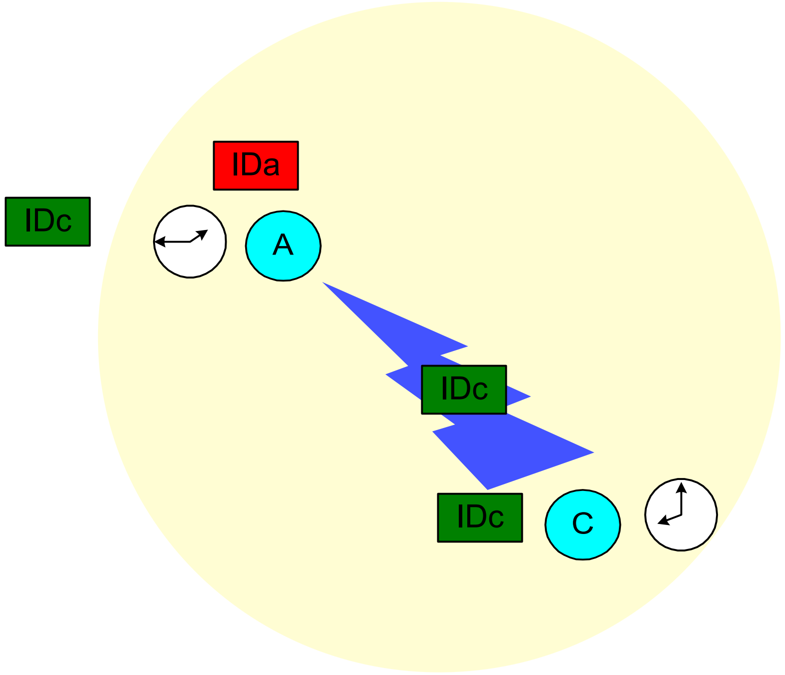
- Paging assumes master has slaves *Device ID* and an idea of its *Clock*

Master Paging a Slave



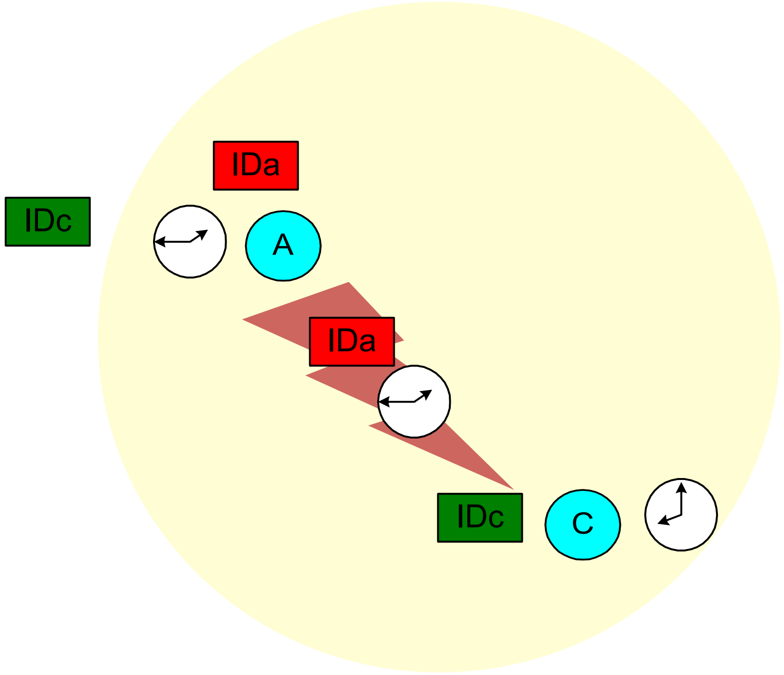
- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - – A pages C with C's *Device ID* and CLKE

Master Paging a Slave



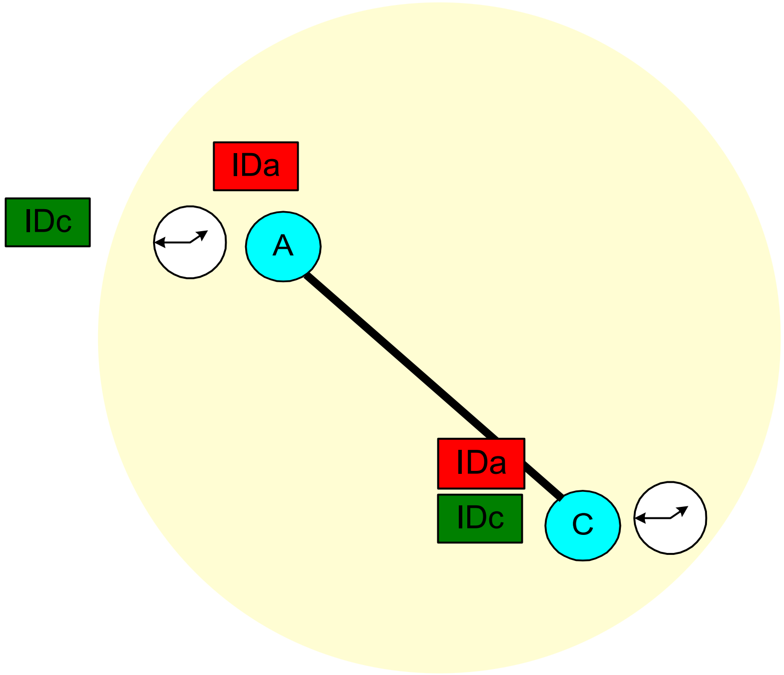
- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - A pages C with C's *Device ID* (DAC)
  - C Replies to A with C's *Device ID*

Master Paging a Slave



- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - A pages C with C’s *Device ID*
  - C Replies to A with C’s *Device ID*
  - A sends C its *Device ID* and *Clock* (FHS packet)

Master Paging a Slave



- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - A pages C with C's *Device ID*
  - C Replies to A with C's *Device ID*
  - A sends C its *Device ID* and *Clock* (FHS packet)
  - A connects as a master to C

Contents

- Bluetooth
  - History and Introduction
  - IEEE 802.15.1
    - Application, Frequency, Architecture, and Protocol Stack
  - IEEE 802.15.3
  - IEEE 802.15.4
- IEEE 802.16: (Worldwide Interoperability for Microwave Access) WiMax

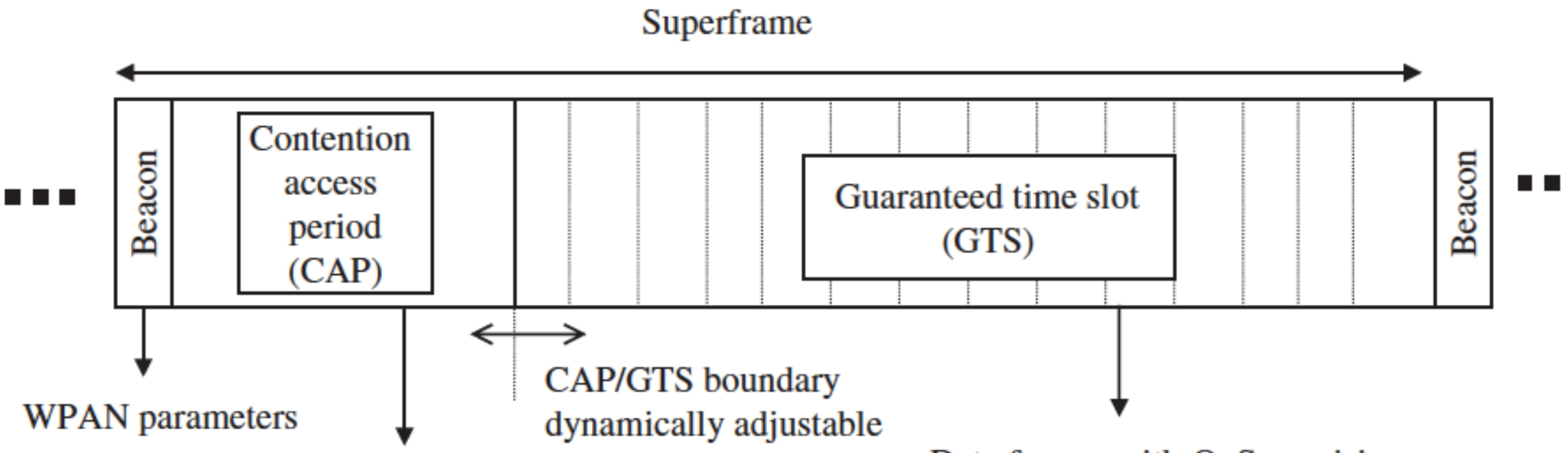
High data rate

IEEE 802.15.3

IEEE 802.15.3

- Ad hoc MAC layer suitable for **multimedia** WPAN applications
- A PHY capable of data rates in excess of **20 Mbps**
- MAC **superframe** structure
  - **A network beacon interval**
  - **A contention access period (CAP)**
    - The CAP period is reserved for transmitting non-QoS data frames such as short bursty data or channel access requests made by the devices in the network
  - **Guaranteed time slots (GTSs)**
    - The type of data transmitted in the GTS can range from bulky image or music files to high-quality audio or high-definition video streams.

IEEE 802.15.3 MAC Superframe



WPAN parameters

CAP/GTS boundary dynamically adjustable

Non-QoS data frames:
- Short bursty data
- Channel access requests

Data frames with QoS provisions:
- Image files
- MP3 music files (multimedia files)
- Standard definition MPEG2, 4.5 Mb/s
- High-definition MPEG2, 19.2 Mb/s
- MPEG1, 1.5 Mb/s
- DVD, up to 9.8 Mb/s
- CD audio, 1.5 Mb/s
- AC3 Dolby digital, 448 Kb/s
- MP3 streaming audio, 128 Kb/s

Contents

- Bluetooth
  - – History and Introduction
  - – IEEE 802.15.1
    - Application, Frequency, Architecture, and Protocol Stack
  - – IEEE 802.15.3
  - – IEEE 802.15.4
- IEEE 802.16: (Worldwide Interoperability for Microwave Access) WiMax

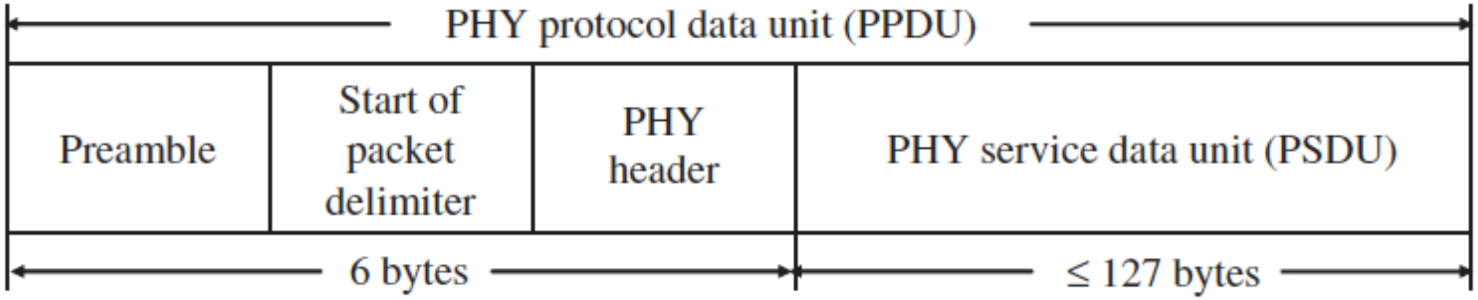
Low data rate and low power

IEEE 802.15.4

IEEE 802.15.4

- Defines a specification for low-rate, low-power WPANs
  - PC peripherals:
    - keyboards, wireless mice, low-end PDAs, and joysticks;
  - Consumer electronics:
    - radios, TVs, DVD layers, and remote controls;
  - Home automation:
    - heating, ventilation, air conditioning, security, lighting, and control of windows, curtains, doors, locks
  - Health monitors and diagnostics
- **Zigbee** alliance which includes **Philips, Honeywell and Invensys Metering** Systems and **IEEE 802.15.4 Standard**

IEEE 802.15.4 PHY Layer Packets



PHY protocol data unit (PPDU)

Preamble	Start of packet delimiter	PHY header	PHY service data unit (PSDU)

6 bytes

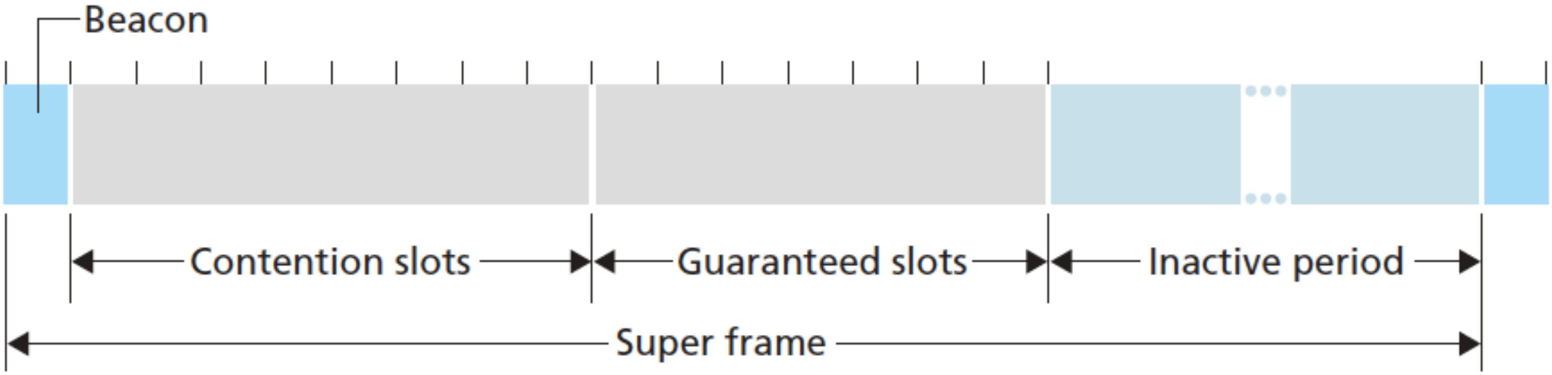
≤ 127 bytes

PHY packet fields:

- Preamble (32 bits) synchronization
- Start of packet delimiter (8 bits) signifies end of preamble
- PHY header (8 bits) specifies length of PSDU
- PSDU (≤ 127 bytes) PHY layer payload

Zigbee: 802.15.4

- Zigbee is targeted at lower powered, lower-data-rate, lower-duty-cycle
- Examples: Home temperature and light sensors, security devices, and wall mounted switches
- Defines channel rates of 20, 40, 100, and 250 Kbps
- “Reduced-Function Devices” versus “Full-Function Devices”



Zigbee 802.15.4 Super-Frame Structure

Contents

- Bluetooth
  - History and Introduction
  - IEEE 802.15.1
    - Application, Frequency, Architecture, and Protocol Stack
  - IEEE 802.15.3
  - IEEE 802.15.4
- IEEE 802.16: (Worldwide Interoperability for Microwave Access) WiMax

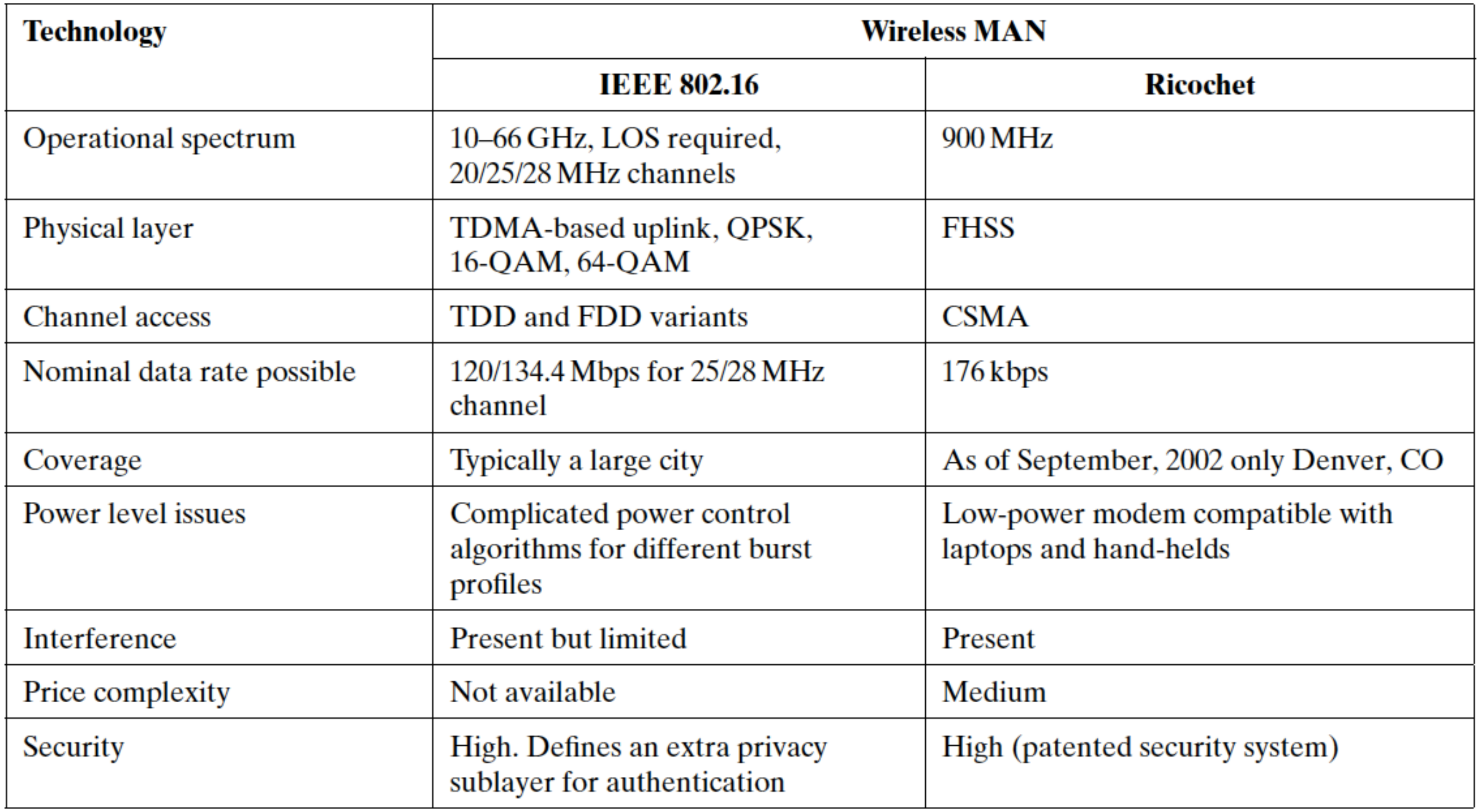
WiMax

IEEE 802.16

IEEE 802.16 Standards

Standard	Scope
IEEE 802.16	Medium Access Control: one common MAC for wireless MAN standards PHY layer: 10 to 66 GHz
IEEE 802.16a	MAC modifications to 802.16.1 PHY Layer: 2 to 11 GHz
IEEE 802.16c	Detailed System Profiles for 10-66 GHz
IEEE 802.16e	Physical and MAC layer for Combined Fixed and Mobile Operation in Licensed Band
IEEE 802.16.2	Coexistence of Fixed Broadband Wireless Access Systems

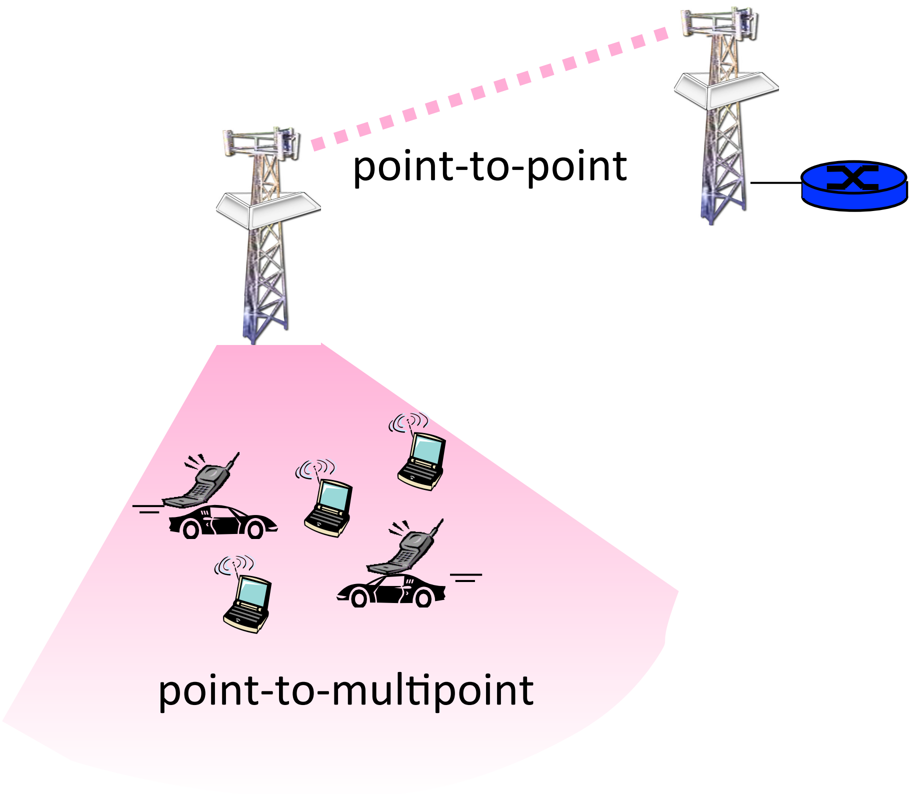
WMAN Standards

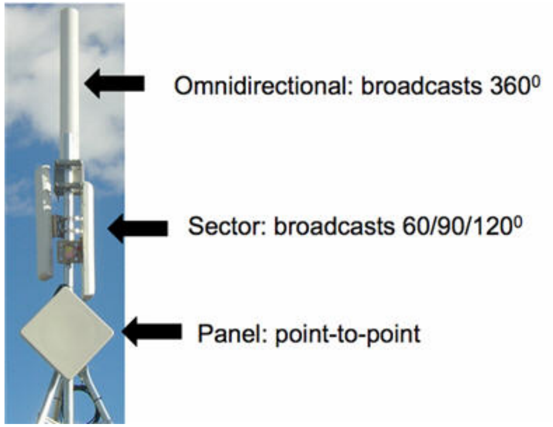


Technology	Wireless MAN	
	IEEE 802.16	Ricochet
Operational spectrum	10–66 GHz, LOS required, 20/25/28 MHz channels	900 MHz
Physical layer	TDMA-based uplink, QPSK, 16-QAM, 64-QAM	FHSS
Channel access	TDD and FDD variants	CSMA
Nominal data rate possible	120/134.4 Mbps for 25/28 MHz channel	176 kbps
Coverage	Typically a large city	As of September, 2002 only Denver, CO
Power level issues	Complicated power control algorithms for different burst profiles	Low-power modem compatible with laptops and hand-helds
Interference	Present but limited	Present
Price complexity	Not available	Medium
Security	High. Defines an extra privacy sublayer for authentication	High (patented security system)

802.16: WiMAX

- like 802.11 & cellular: base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11:
  - range ~ 6 miles ("city rather than coffee shop")
  - ~14 Mbps

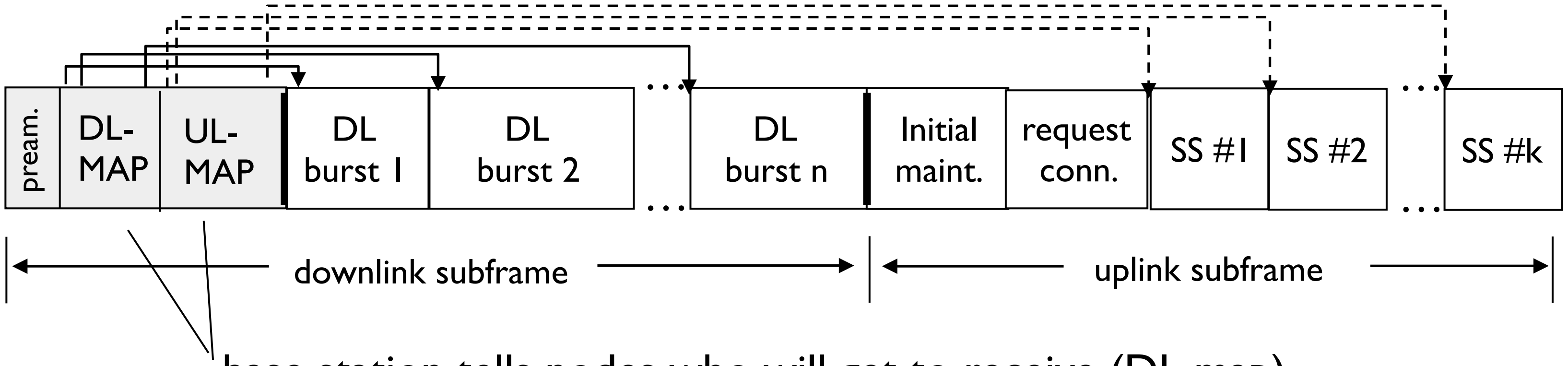



Omnidirectional: broadcasts 360^0
Sector: broadcasts $60/90/120^0$
Panel: point-to-point

WiMAX: World Interoperability for Microwave Access

802.16: WiMAX: downlink, uplink scheduling

- Transmission frame
  - down-link subframe: base station to node
  - uplink subframe: node to base station



base station tells nodes who will get to receive (DL map) and who will get to send (UL map), and when

- WiMAX standard provides mechanism for scheduling, but not scheduling algorithm