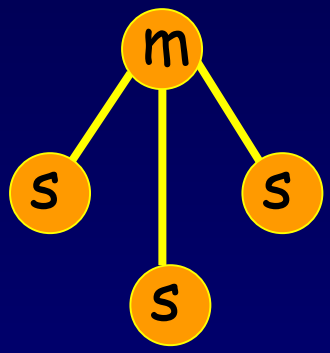


Bluetooth Vs. 802.11

Pravin Bhagwat

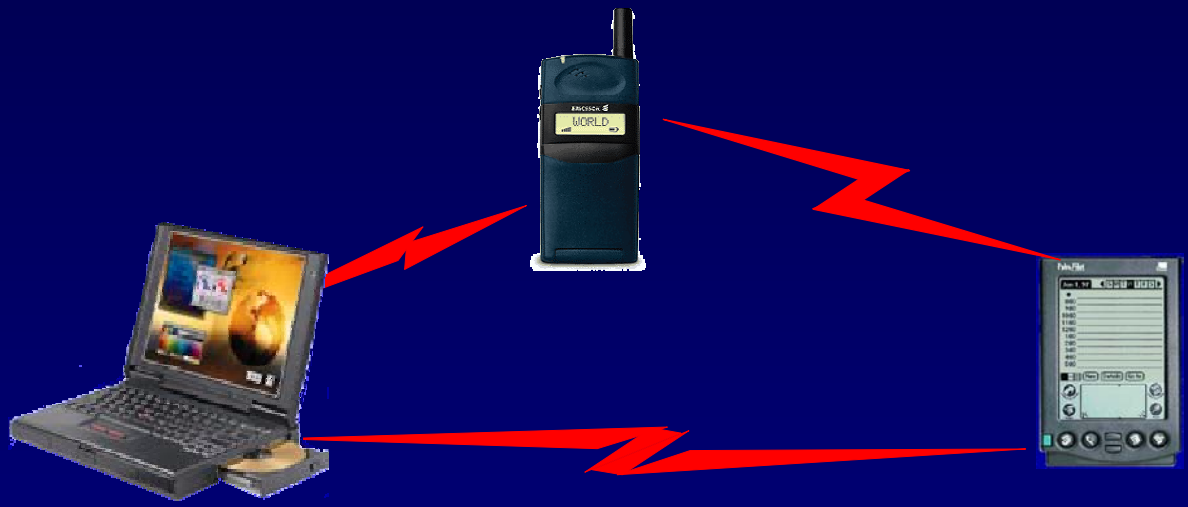
ReefEdge, Inc.

pravin@acm.org

http://www.cs.umd.edu/~pravin

Hot Interconnects
Aug 24, 2001

Bluetooth



- A cable replacement technology
- 1 Mb/s symbol rate
- Range 10+ meters
- Single chip radio + baseband
  - at low power & low price point ($5)

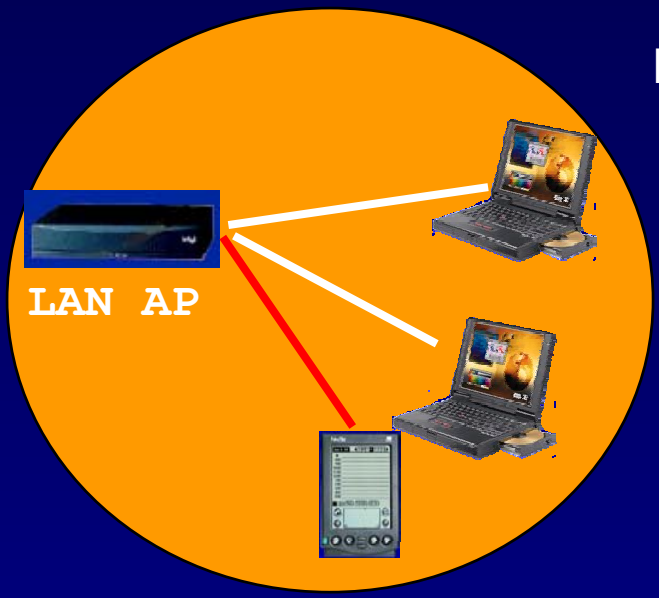
Why not use Wireless LANs?
- power
- cost

802.11

- Replacement for Ethernet
- Supported data rates
  - Current: 11, 5.5, 2, 1 Mbps
  - Future: 20+ Mbps in 2.4 GHz and up to 54 Mbps in 5.7 GHz band
- Range
  - Indoor 20 - 25 meters
  - Outdoor: 50 – 100 meters
- Transmit power up to 100 mW
- Cost:
  - Chipsets $ 35 – 50
  - AP $200 - $1000
  - PCMCIA cards $100 - $150

Emerging Landscape

802.11



New developments are blurring the distinction

- 802.11b for PDAs
- Bluetooth for LAN access

Bluetooth

- Which option is technically superior ?
- What market forces are at play ?
- What can be said about the future ?

Questions I hope to answer

- What are the key design differences between Bluetooth and 802.11 ?
  - At PHY, MAC, and System level
- How do Bluetooth and 802.11 compare ?
  - Cost, Range of communication, performance
- Why is Bluetooth supposed to be low cost and low power ? Can 802.11 achieve the same price and performance target ?
- Is Bluetooth more secure than 802.11 ?
- What is the reality behind the hype ?
- Can the two systems co-exist ?

Tutorial Overview

1:30 – 2:00 pm	Introduction, Bluetooth history, basic radio concepts, Bluetooth RF
2:00 - 2:30 pm	Bluetooth Baseband
2:30 - 3:00 pm	LMP, Security
3:00 - 3:30 pm	SDP, Scatternets
3:30 - 4:00 pm	802.11 specifications overview, PHY
4:00 - 4:30 pm	MAC, WEP
4:30 - 5:00 pm	Comparison, Conclusion

Bluetooth working group history

- February 1998: The Bluetooth SIG is formed
  - promoter company group: Ericsson, IBM, Intel, Nokia, Toshiba
- May 1998: Public announcement of the Bluetooth SIG
- 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
- March 2001: ver. 1.1 is released
- Aug 2001: There are 2,491+ adopter companies

New Applications

Synchronization

User benefits

- Automatic synchronization of calendars, address books, business cards
- Push button synchronization
- Proximity operation

Cordless Headset

User benefits

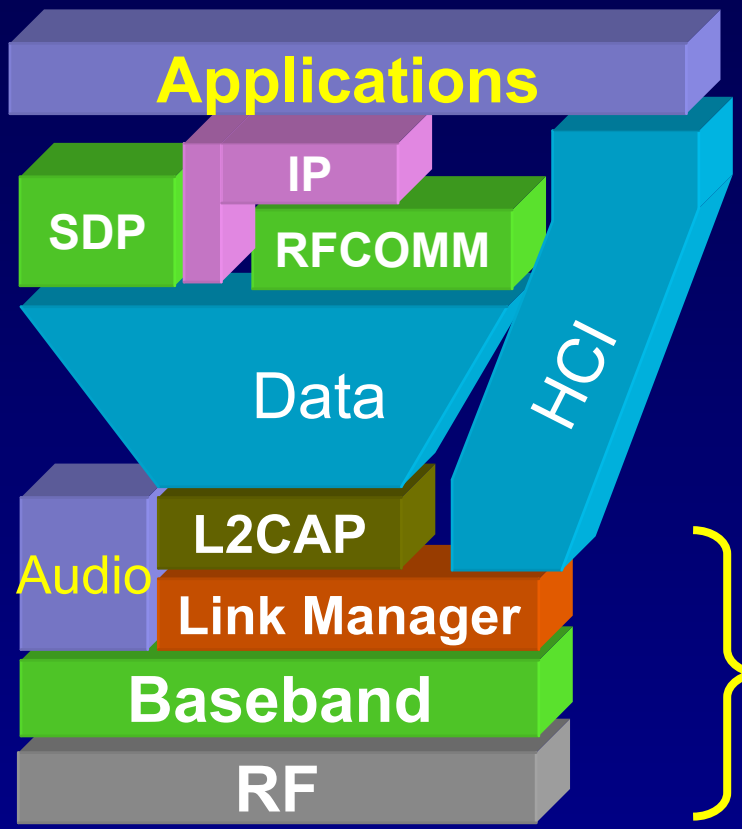
- **Multiple device access**
- **Cordless phone benefits**
- **Hands free operation**

Usage scenarios examples

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

Bluetooth Specifications

Bluetooth Specifications

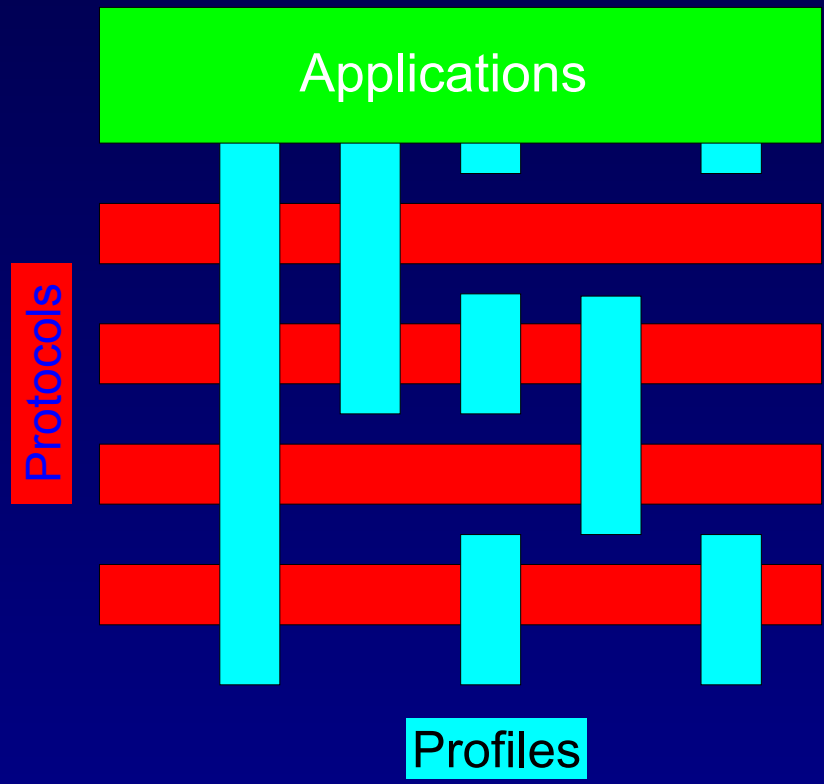


Single chip with RS-232, USB, or PC card interface

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

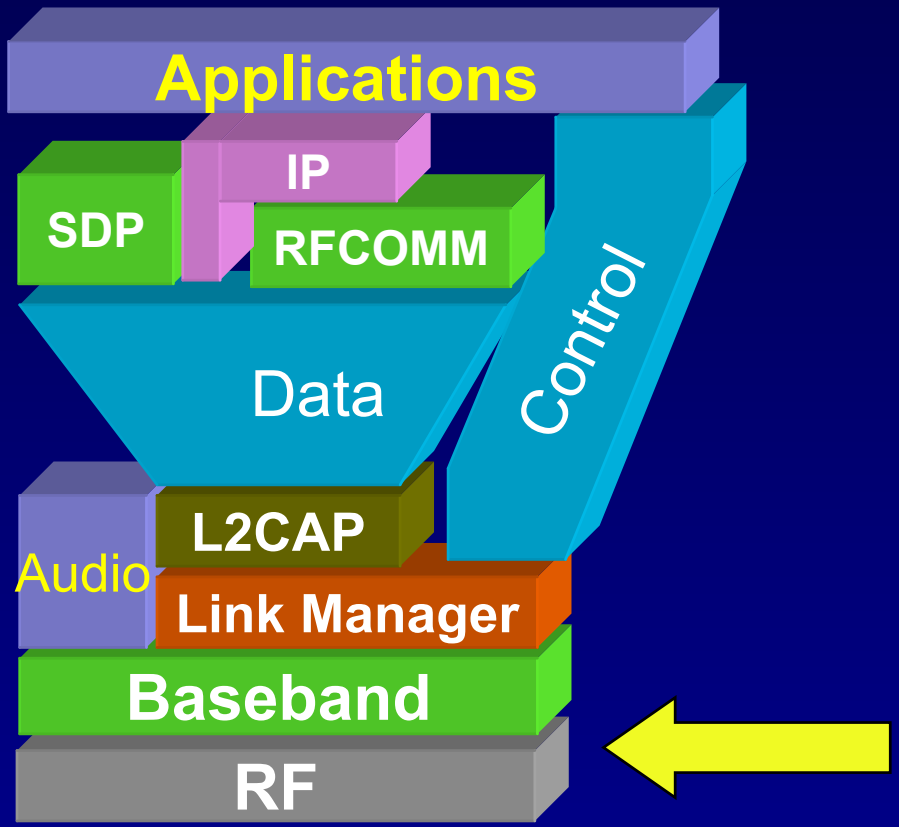
Interoperability & Profiles

- 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

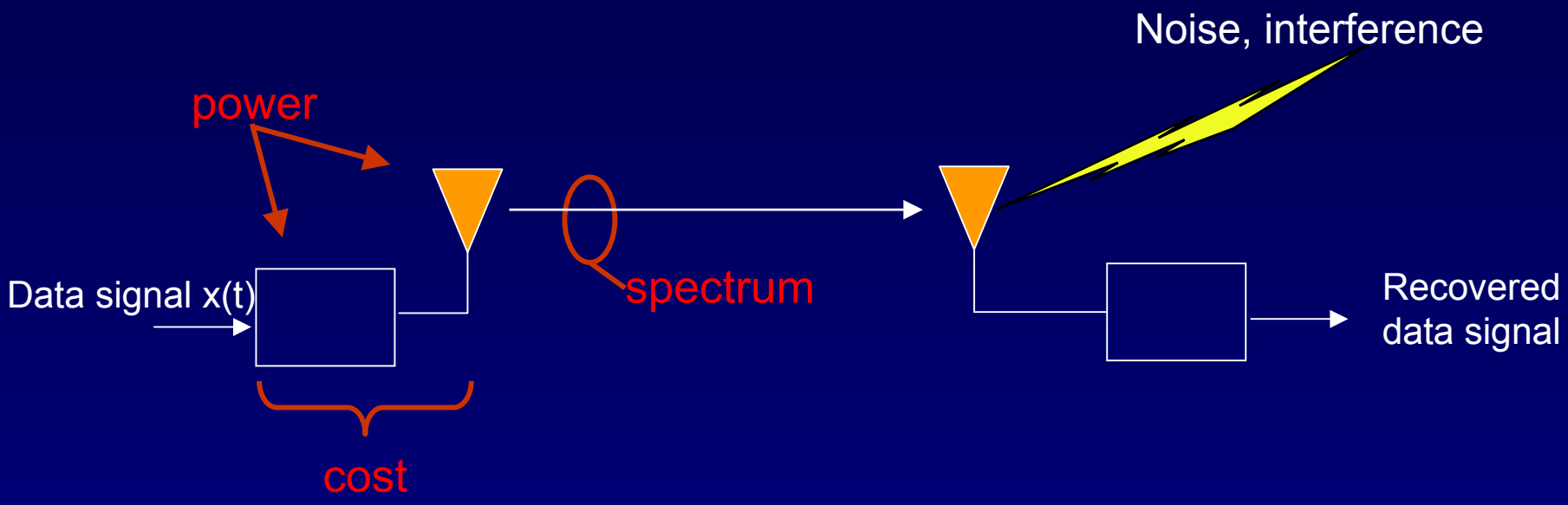


Technical Overview

Bluetooth Radio Specification



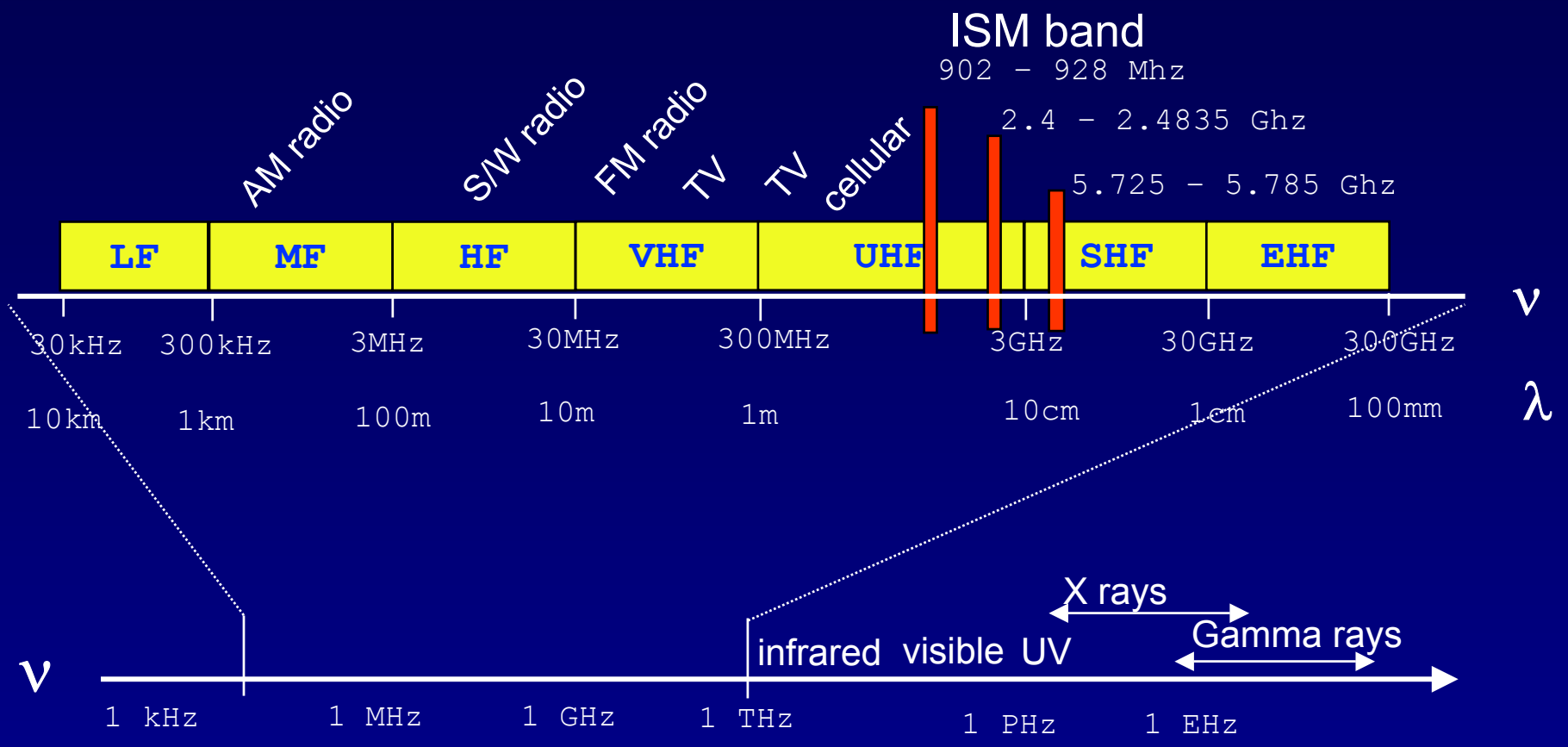
Design considerations



Goal

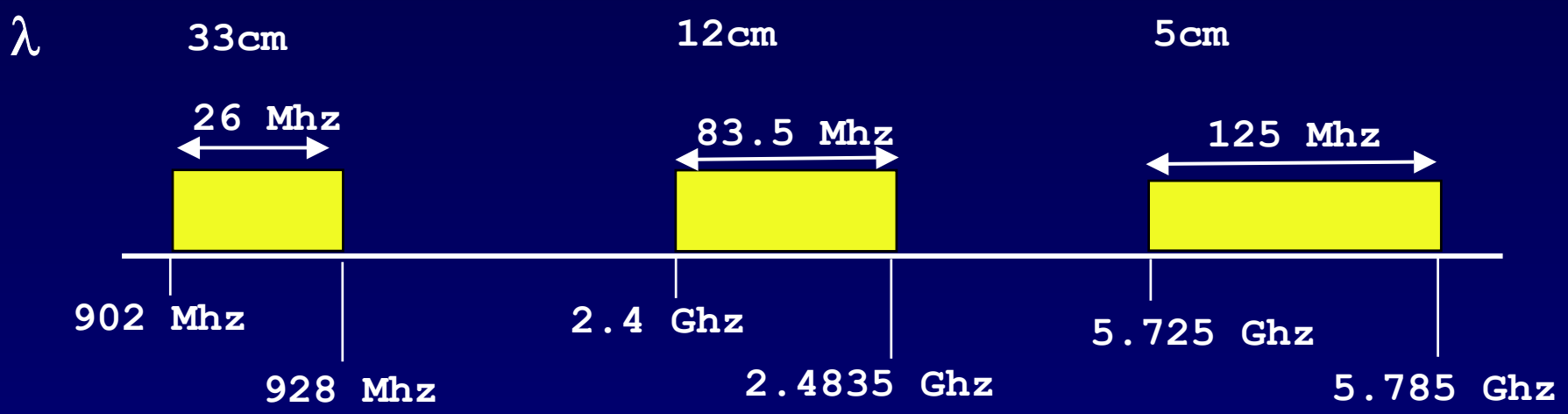
- high bandwidth
- conserve battery power
- cost < $10

EM Spectrum



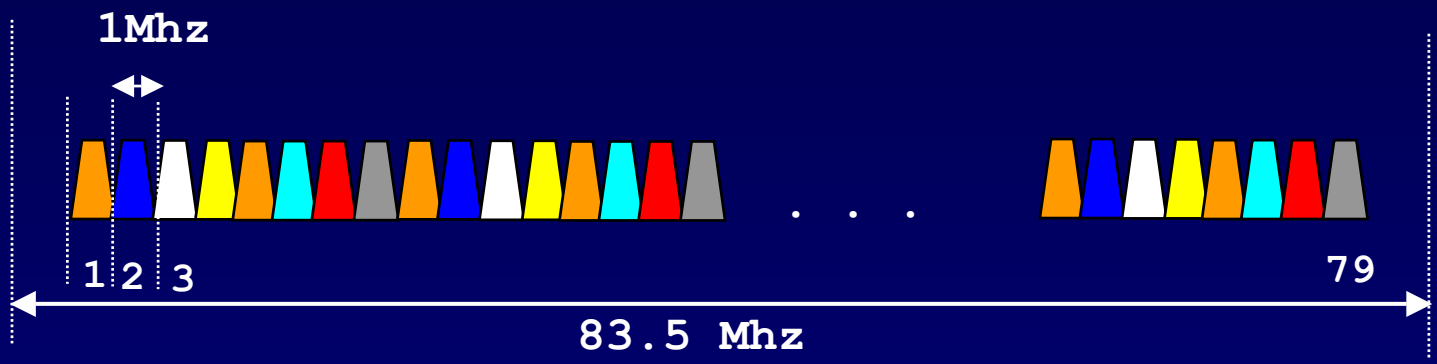
Propagation characteristics are different in each frequency band

Unlicensed Radio Spectrum



cordless phones	802.11	unused
baby monitors	Bluetooth	
Wireless LANs	Microwave oven	

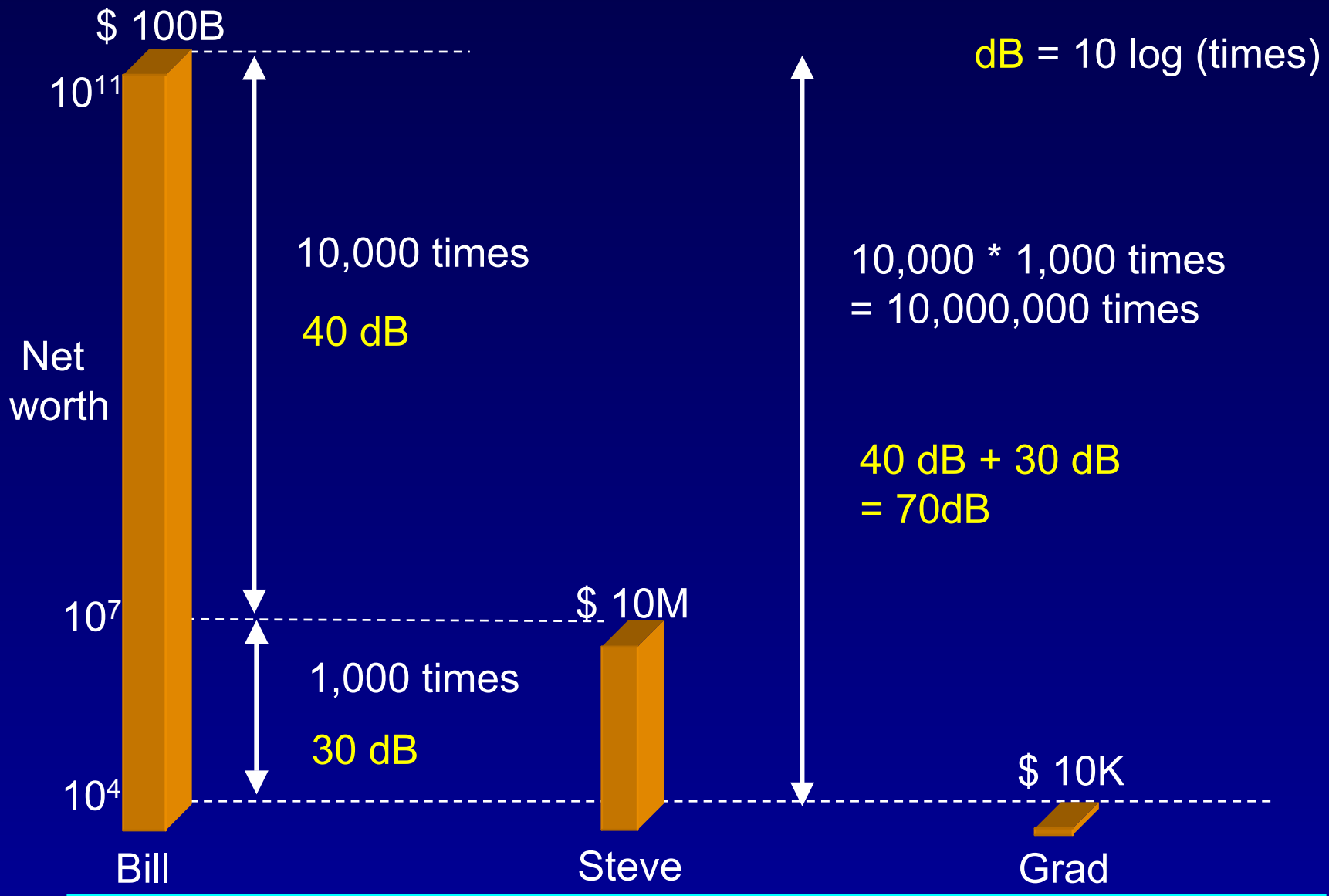
Bluetooth radio link



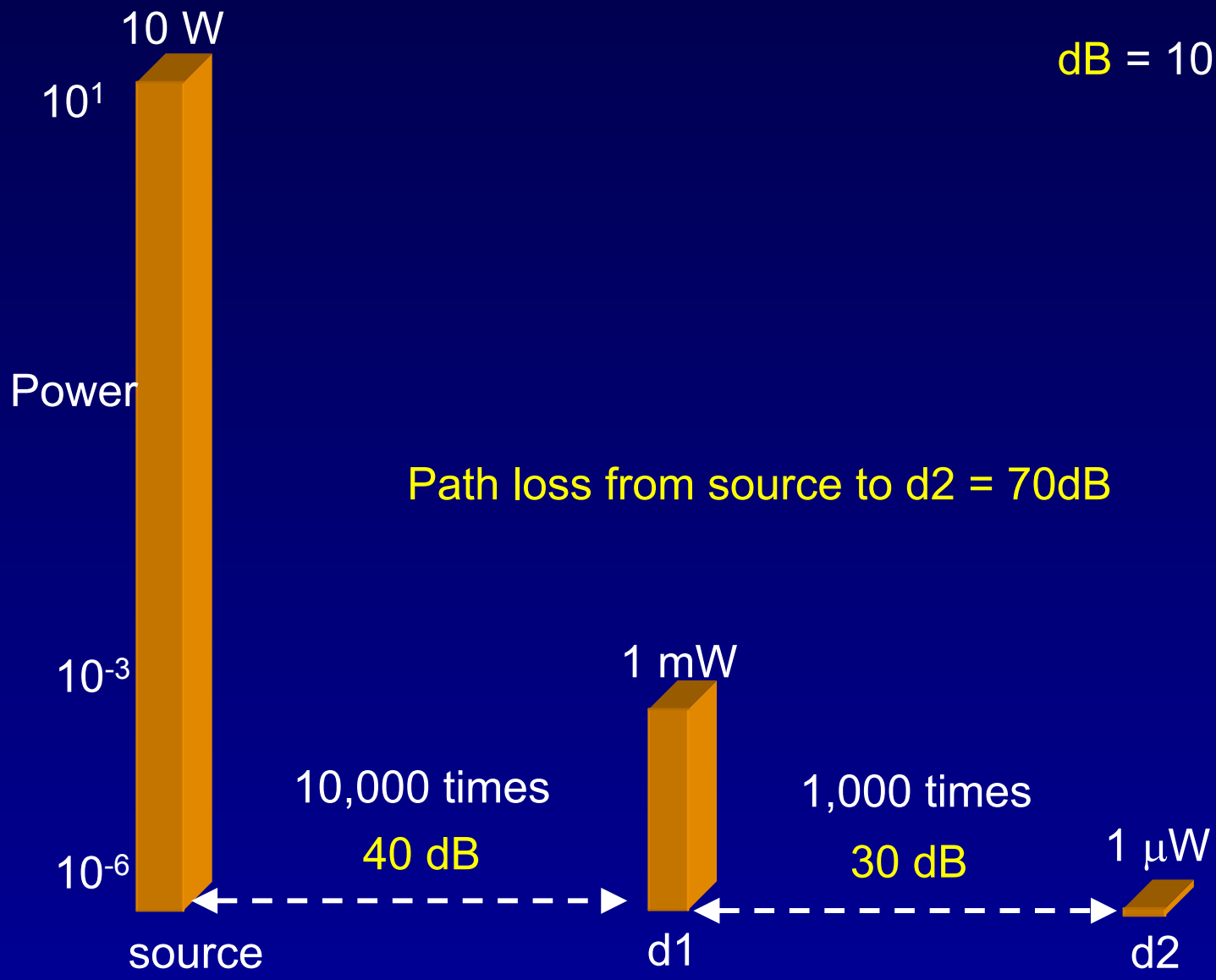
- frequency hopping spread spectrum
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second
- GFSK modulation
  - 1 Mb/s symbol rate
- transmit power
  - 0 dbm (up to 20dbm with power control)

Review of basic concepts

dB (relative measure)



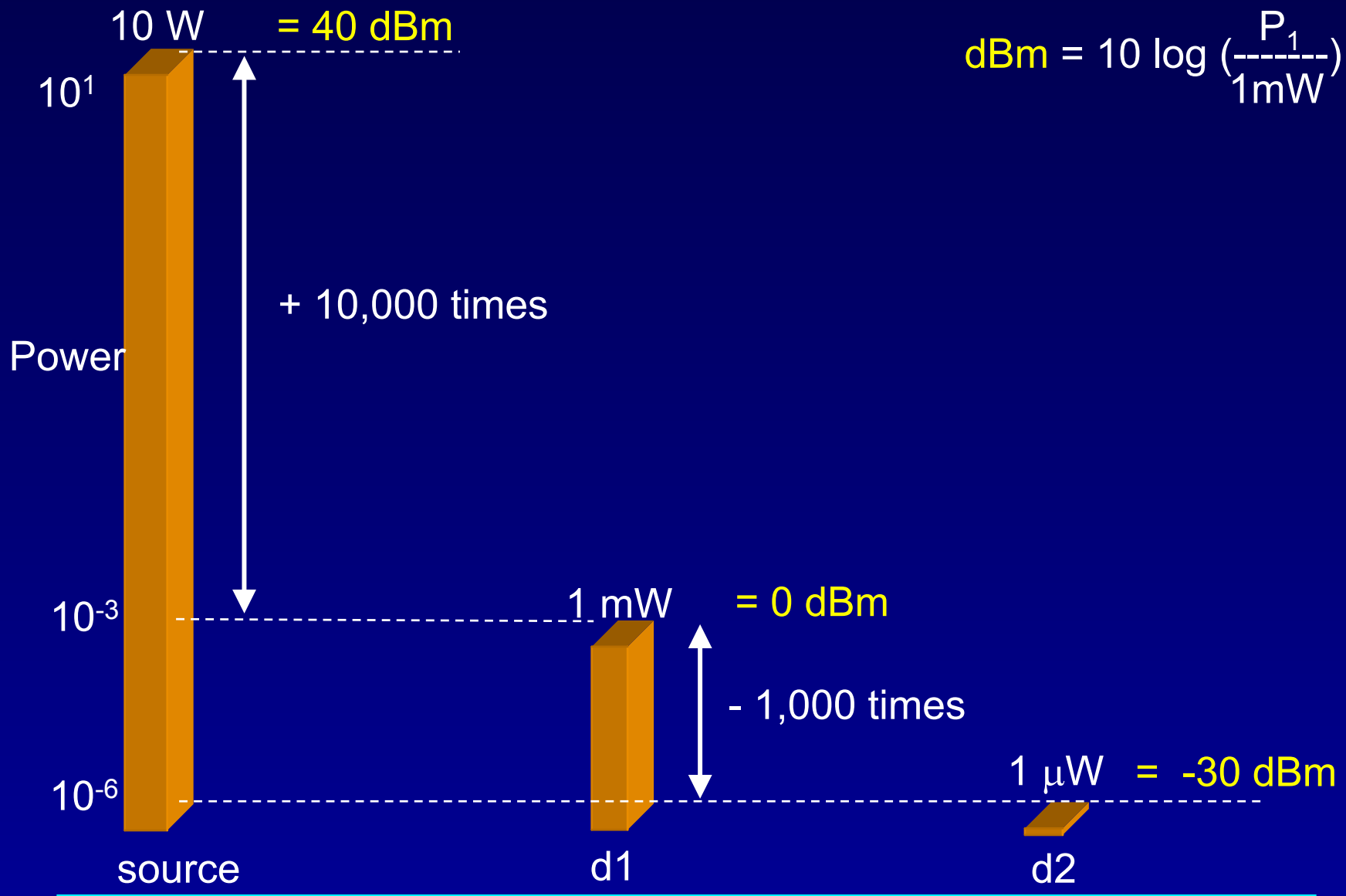
Path loss in dB



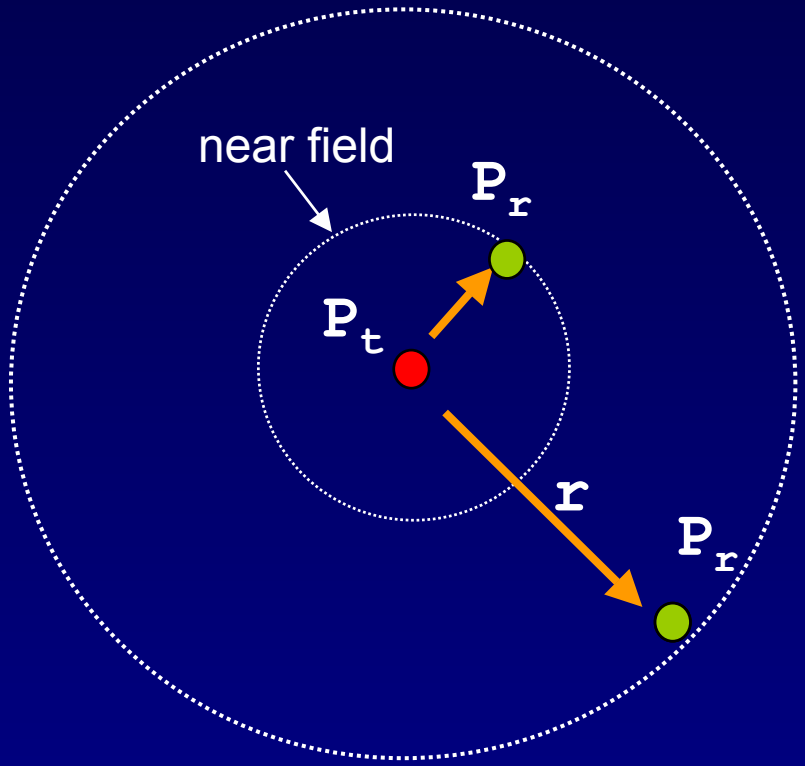
$$dB = 10 \log \left(\frac{P_1}{P_2}\right)$$

Path loss from source to d2 = 70dB

dBm (absolute measure of power)



Radio propagation: path loss



path loss in 2.4 Ghz band

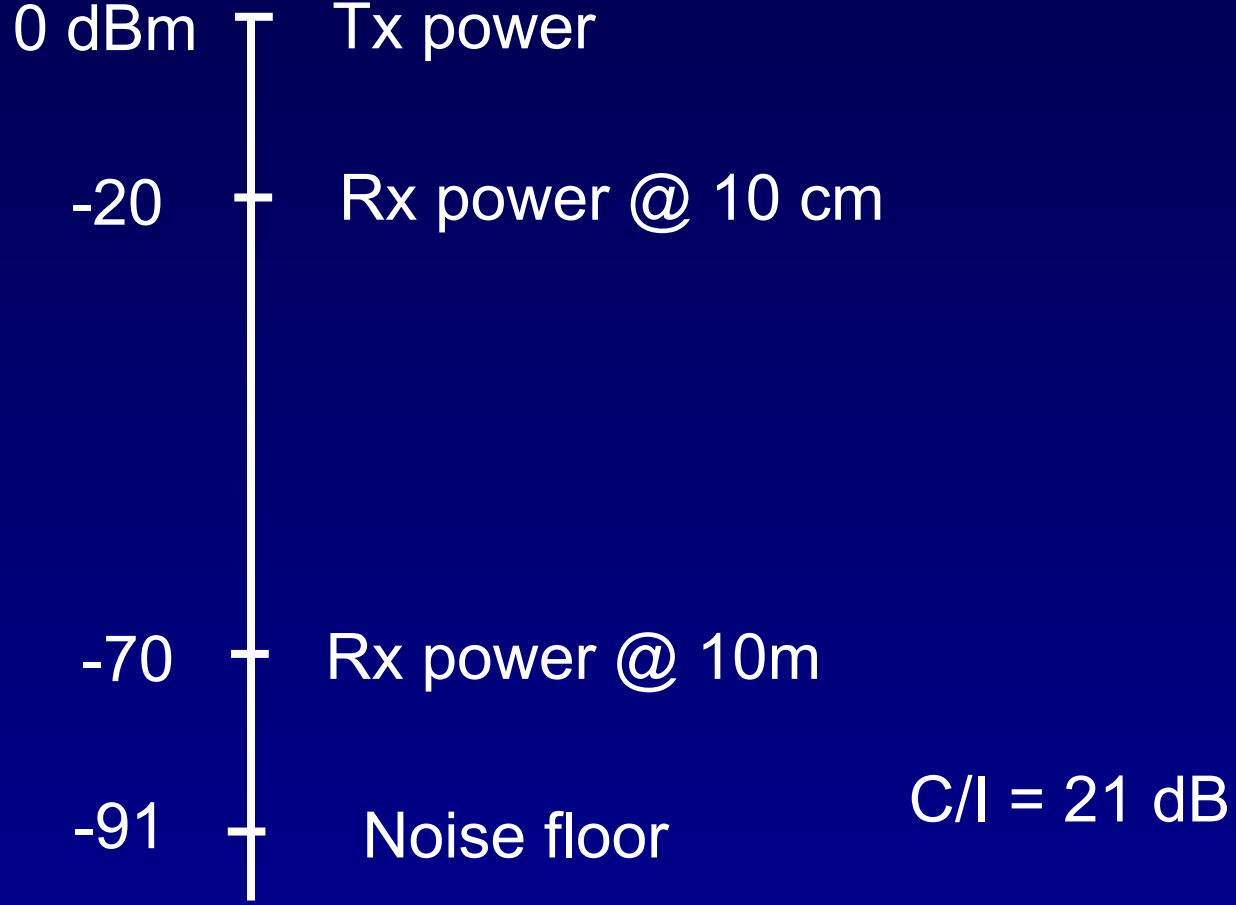
$r \leq 8m$: near field $\propto r^2$

$r > 8m$: far field $\propto r^{3.3}$

path loss $= 10 \log (4\pi r^2/\lambda)$ $\quad r \leq 8m$

$= 58.3 + 10 \log (r^{3.3}/8)$ $\quad r > 8m$

Transmit power & receiver sensitivity



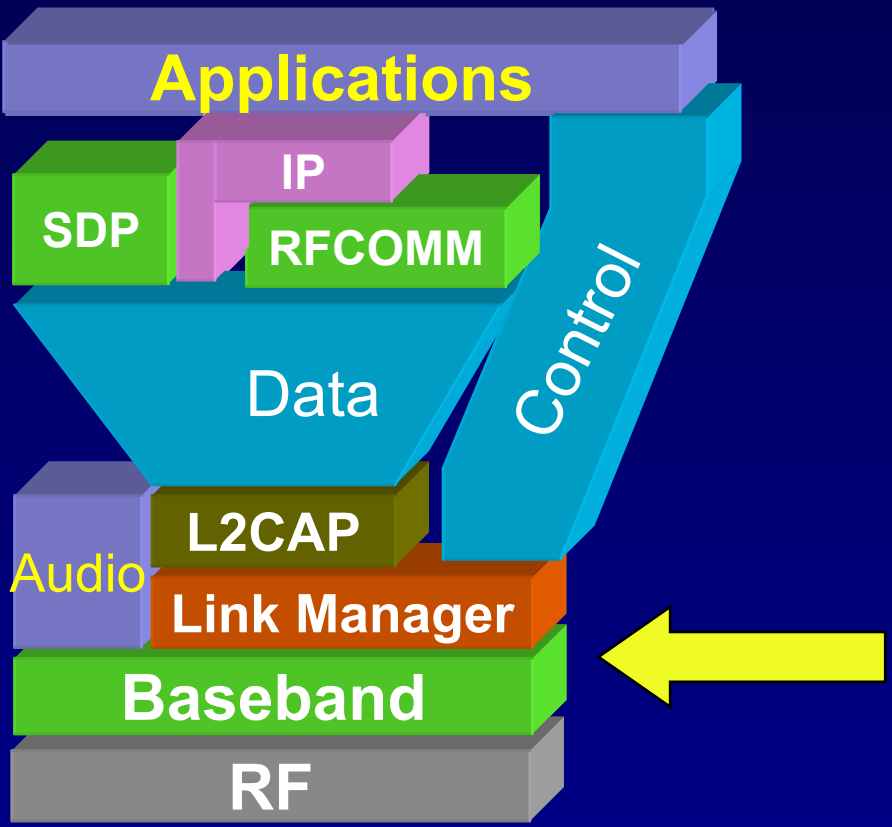
Bluetooth Radio

- 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

Radio: design rationale

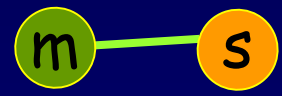
- Allow low cost low IF
- Trade sensitivity for integration
- One chip radio is possible

Baseband

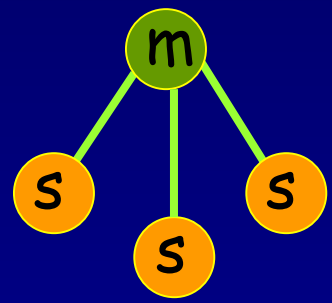

Applications
IP
SDP
RFCOMM
Data
Control
Audio
L2CAP
Link Manager
Baseband
RF

Bluetooth Physical link

- Point to point link
  - master - slave relationship
  - radios can function as masters or slaves

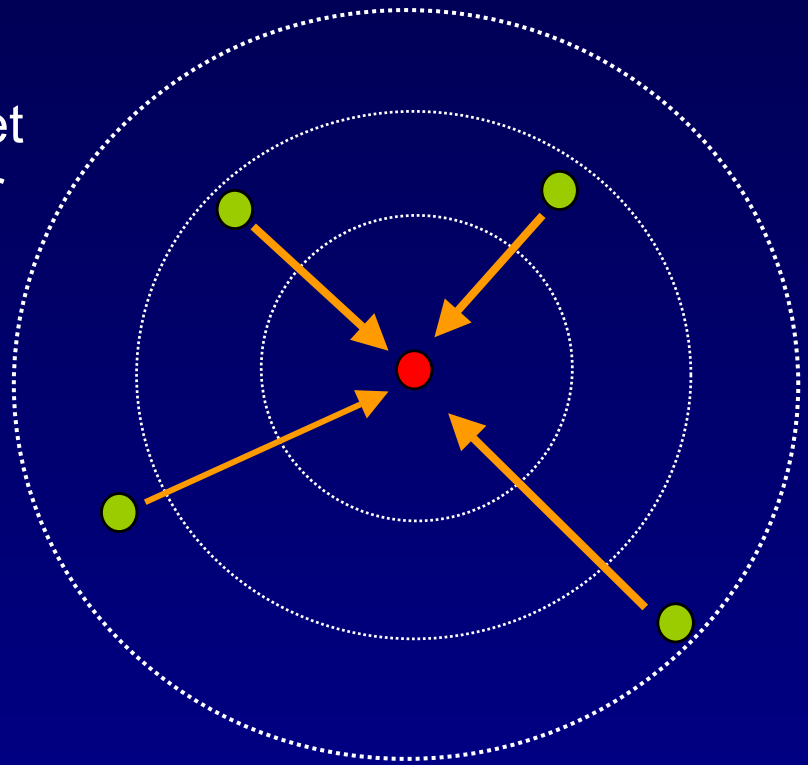


- Piconet
  - Master can connect to 7 slaves
  - Each piconet has max capacity (1 Mbps)
  - hopping pattern is determined by the master

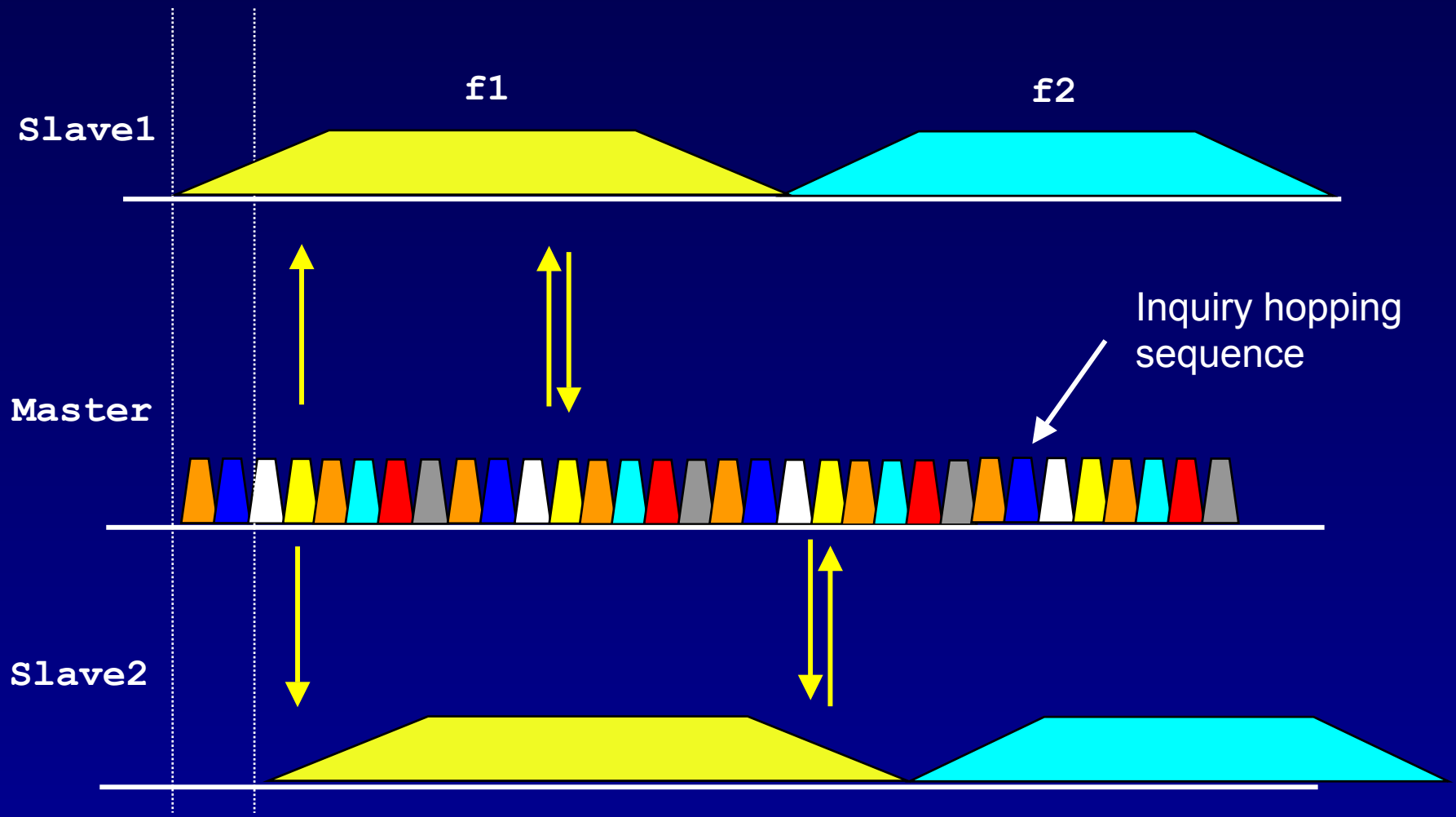


Connection Setup

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

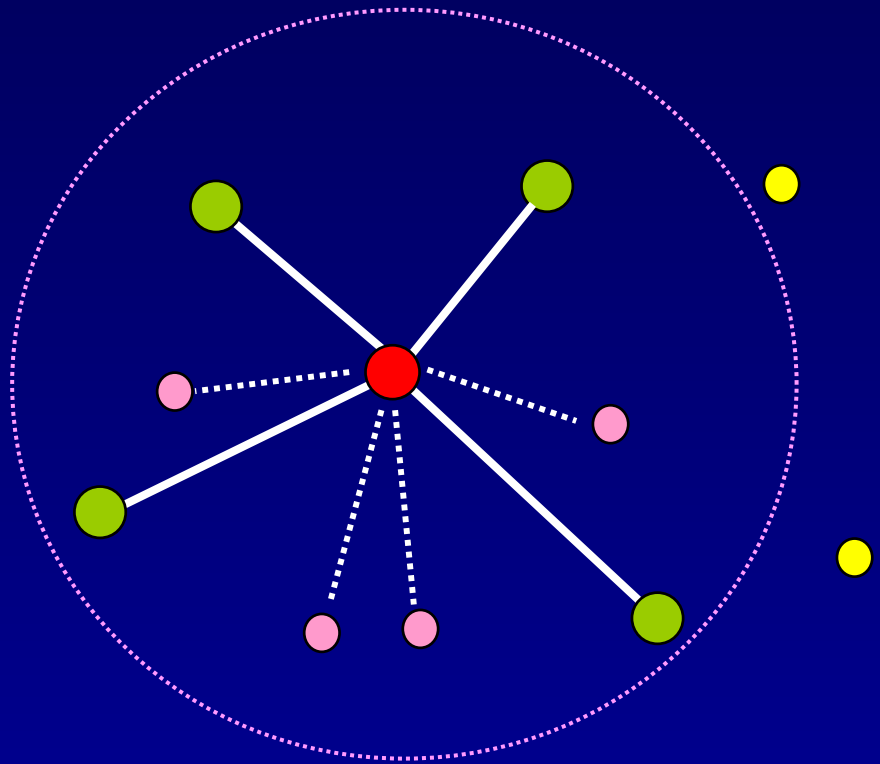


Inquiry on time axis



Piconet formation

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



Master

Active Slave

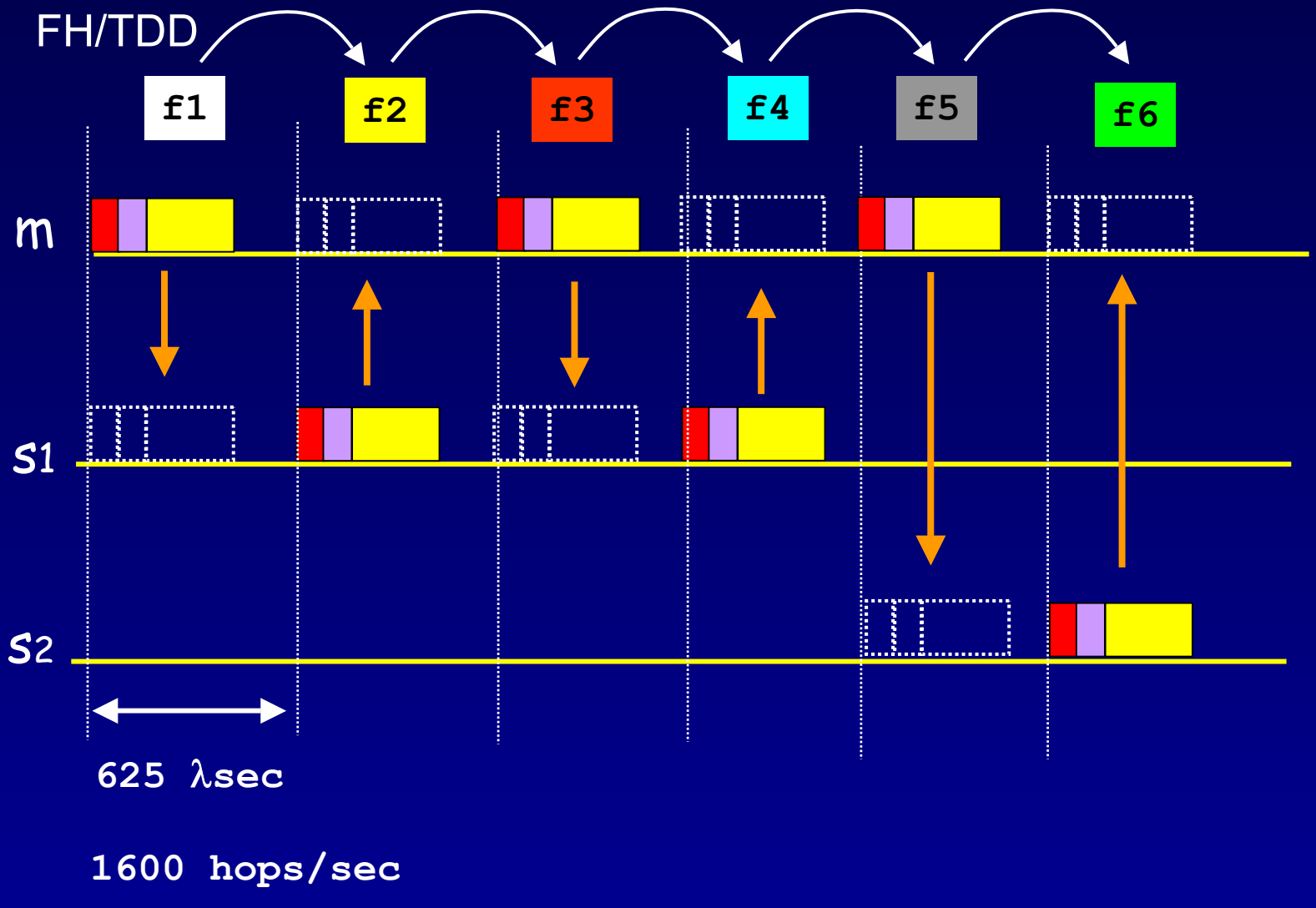
Parked Slave

Standby

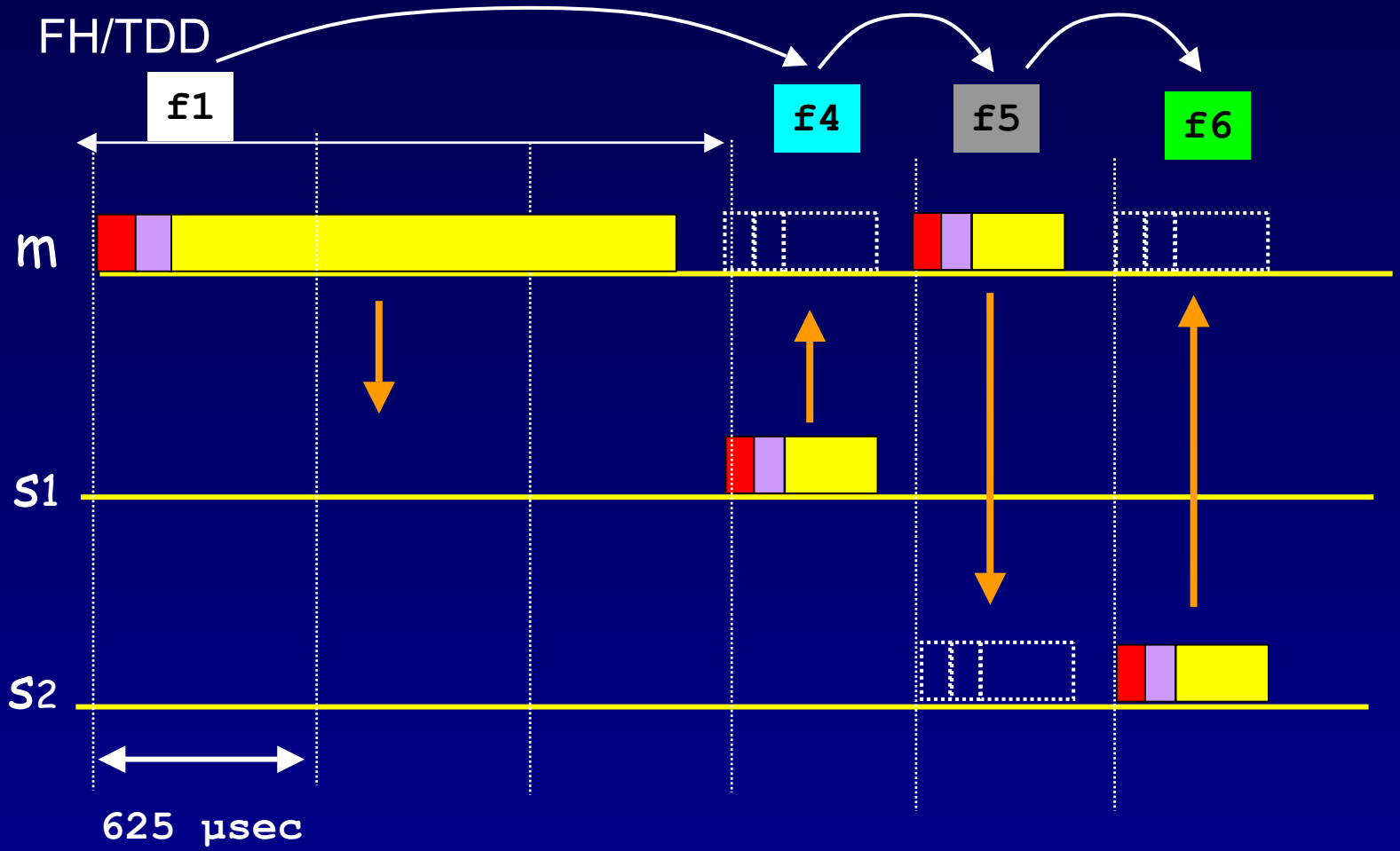
Addressing

- 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



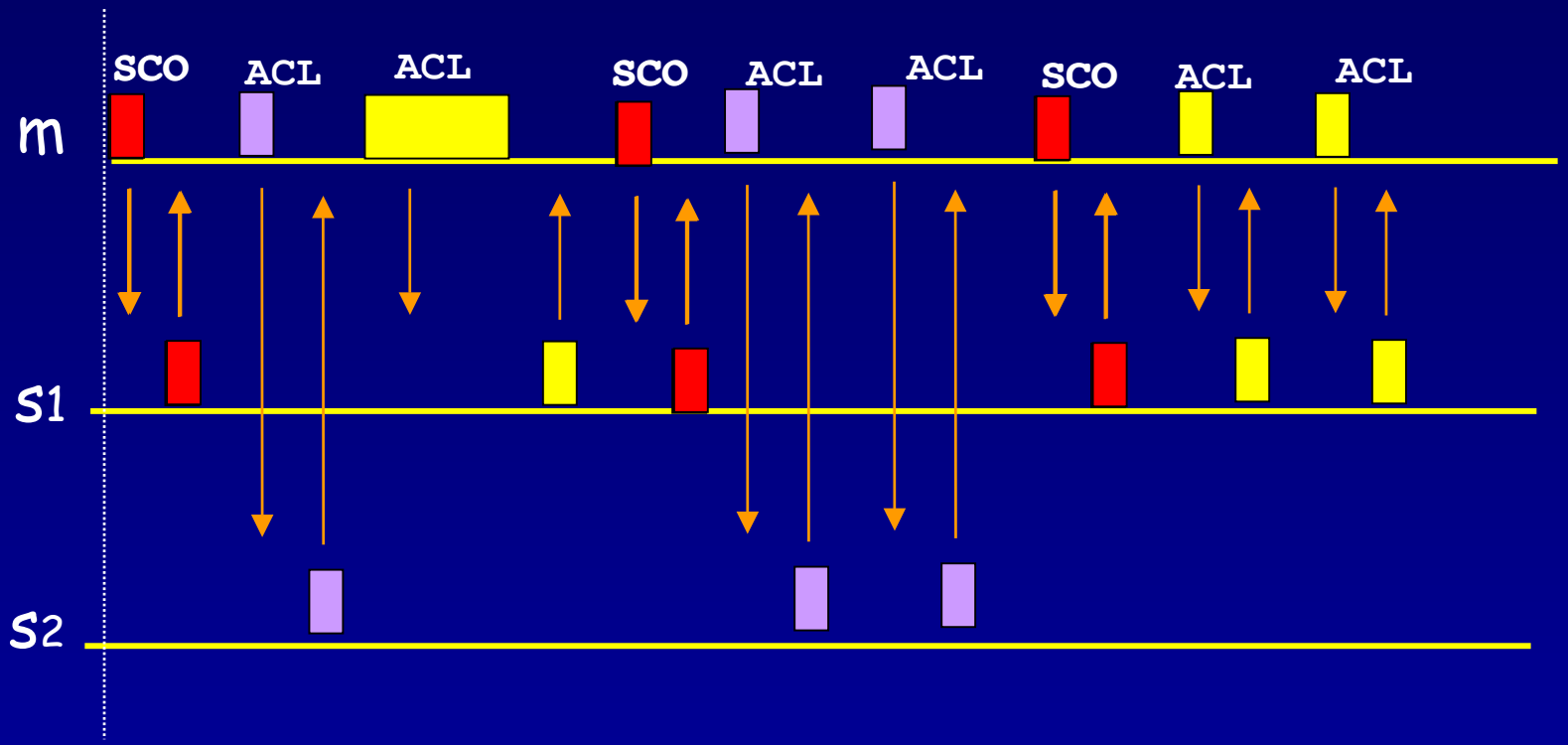
Multi slot packets



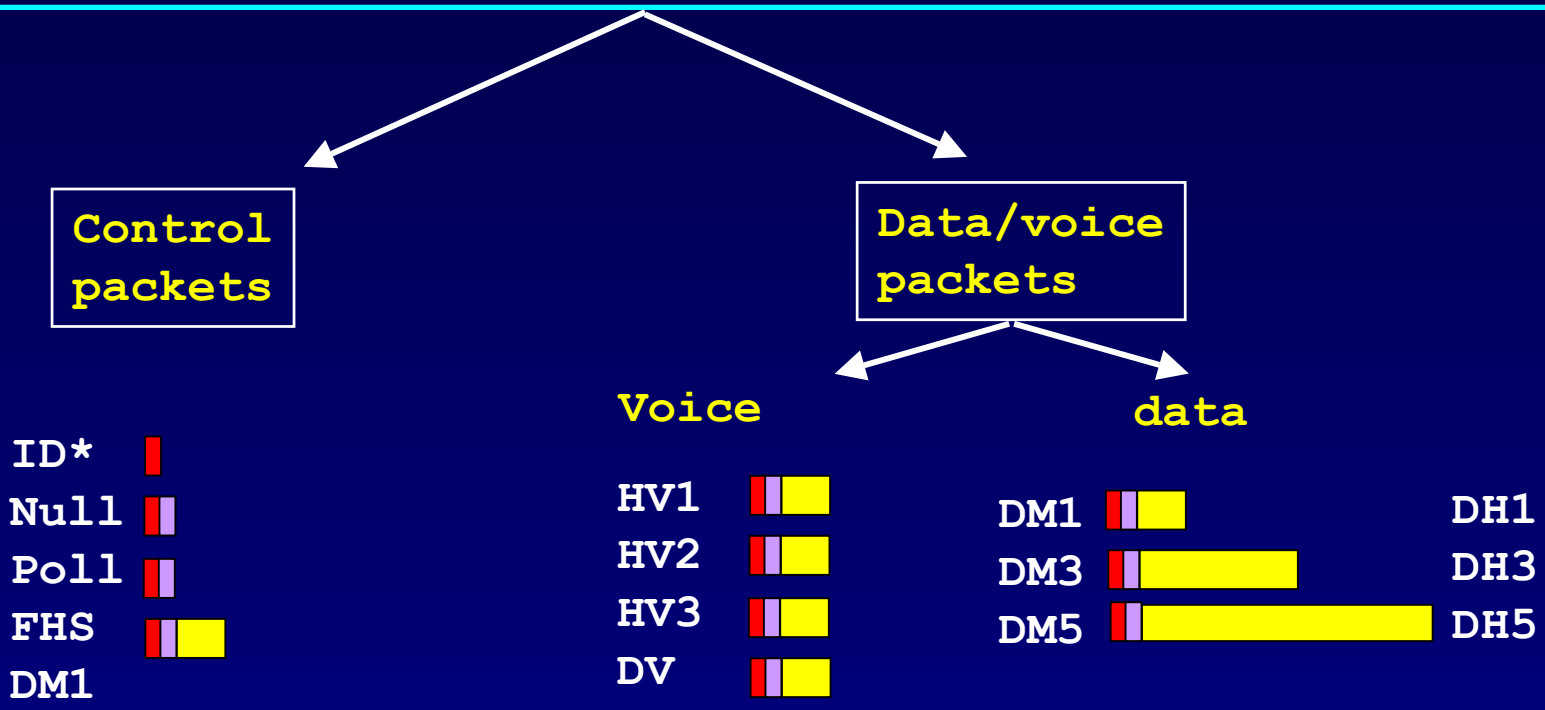
Data rate depends on type of packet

Physical Link Types

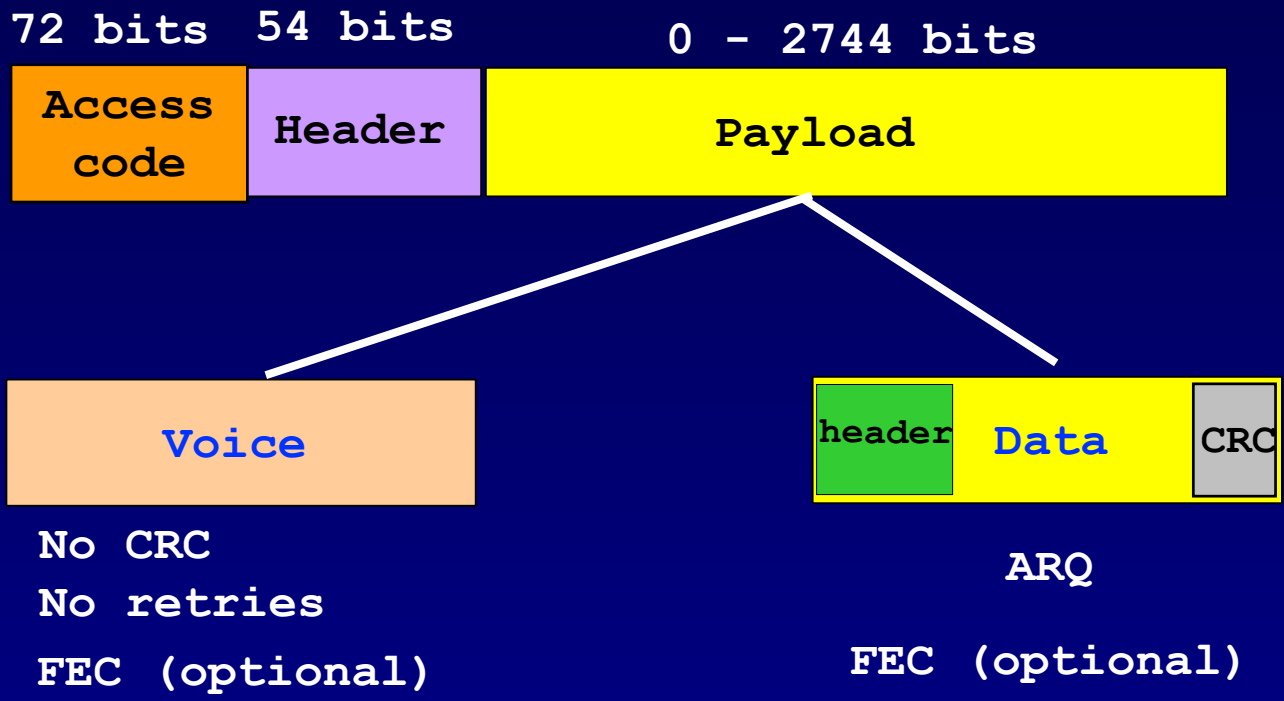
- Synchronous Connection Oriented (SCO) Link
  - slot reservation at fixed intervals
- Asynchronous Connection-less (ACL) Link
  - Polling access method

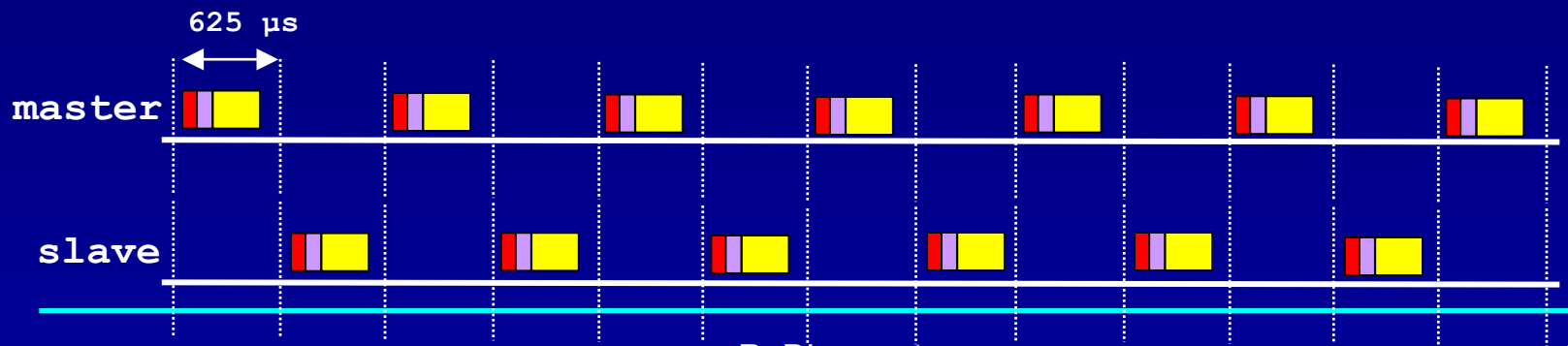


Packet Types

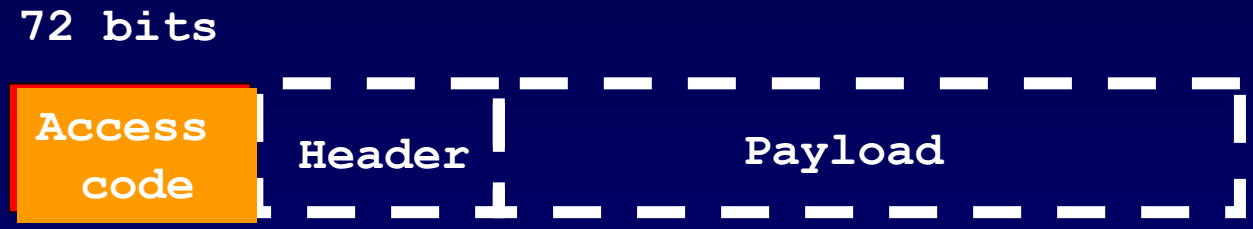


Packet Format





Access Code

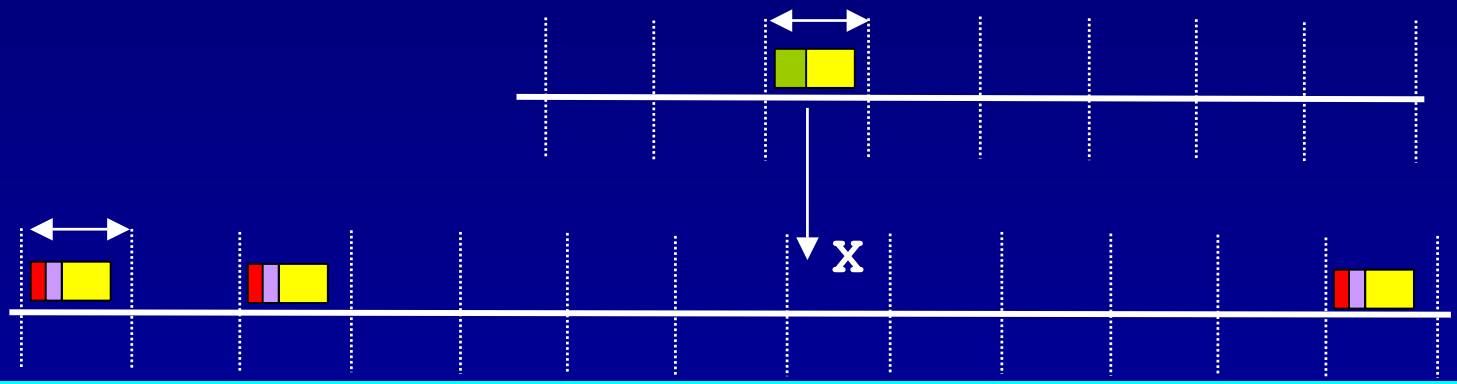


Purpose

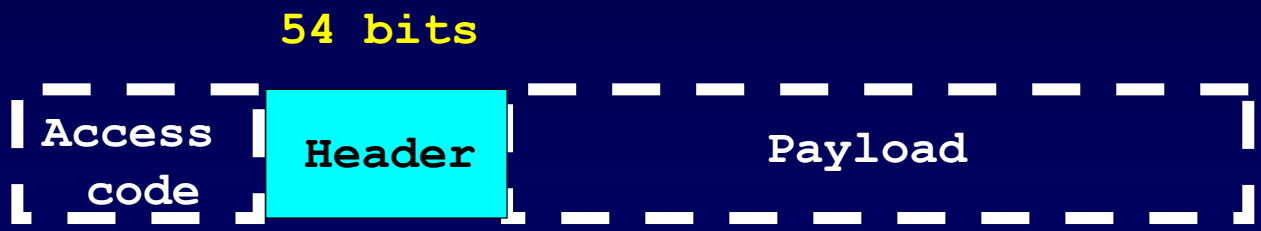
- Synchronization
- DC offset compensation
- Identification
- Signaling

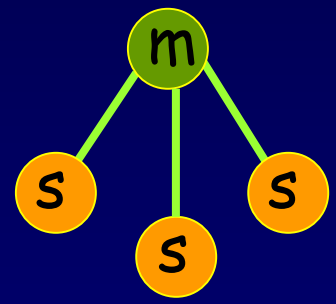
Types

- Channel Access Code (CAC)
- Device Access Code (DAC)
- Inquiry Access Code (IAC)



Packet Header





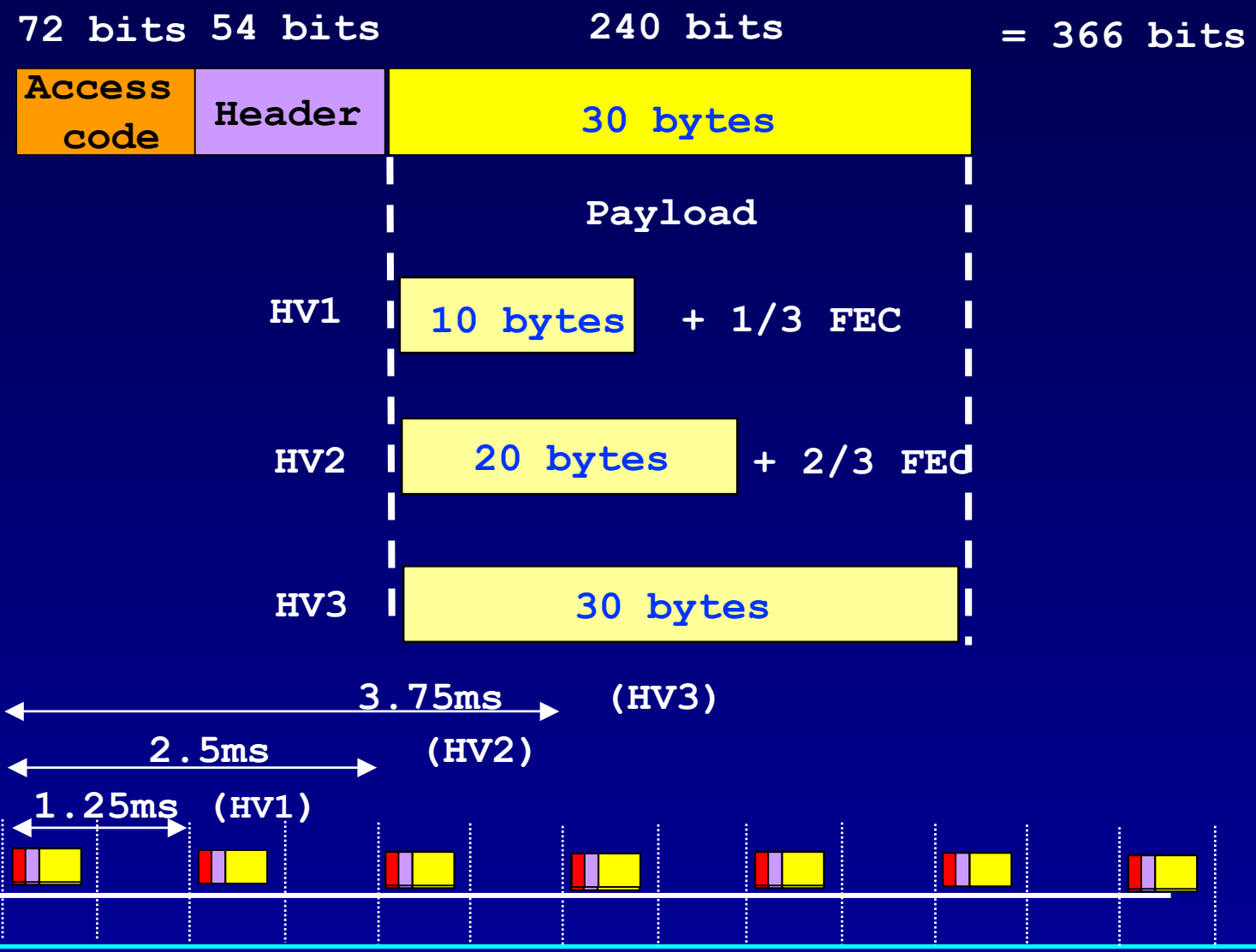
Purpose

- Addressing (3) → Max 7 active slaves
- Packet type (4) → 16 packet types (some unused)
- Flow control (1)
- 1-bit ARQ (1) → Broadcast packets are not ACKed
- Sequencing (1) → For filtering retransmitted packets
- HEC (8) → Verify header integrity

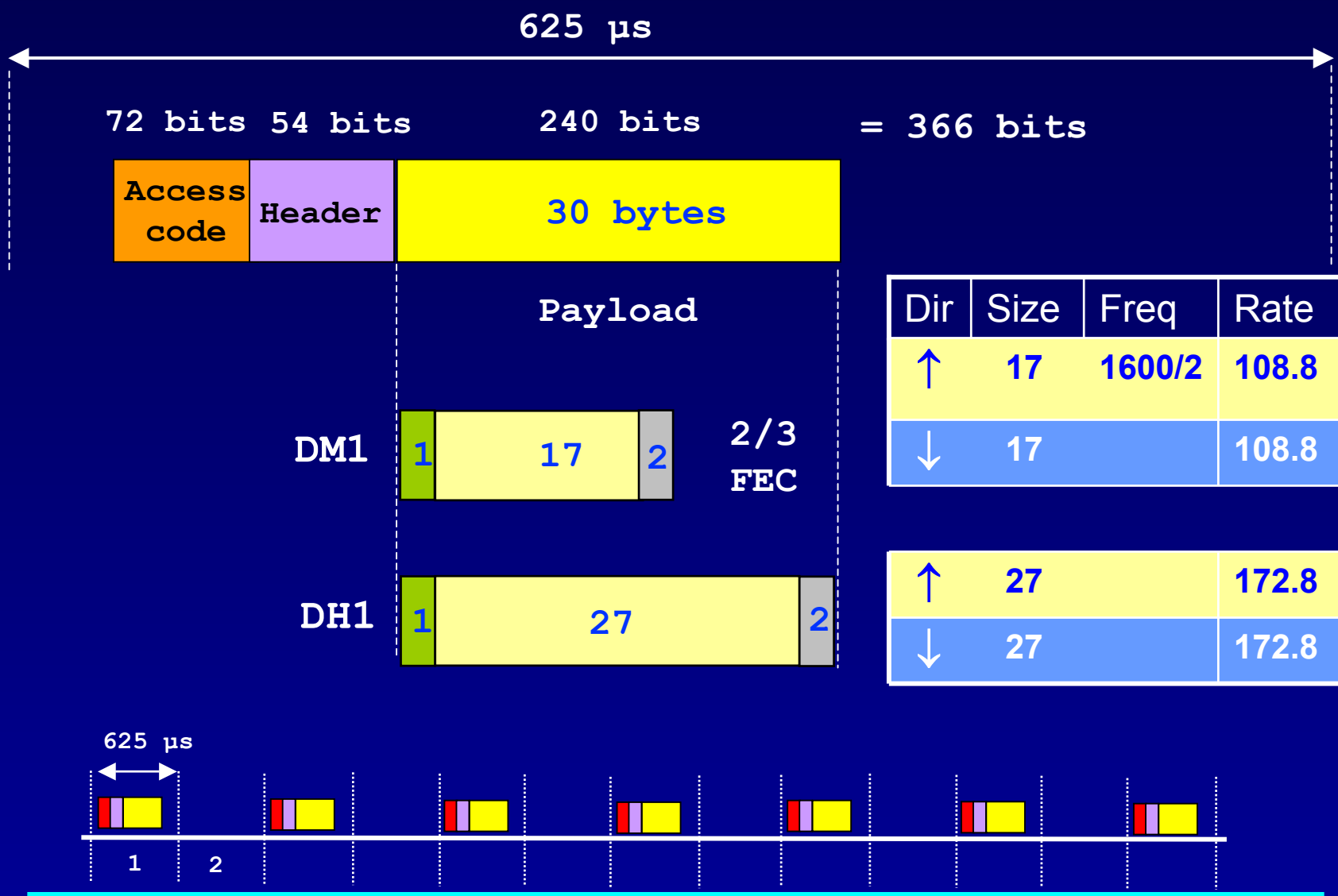
total	18 bits

Encode with 1/3 FEC to get 54 bits

Voice Packets (HV1, HV2, HV3)



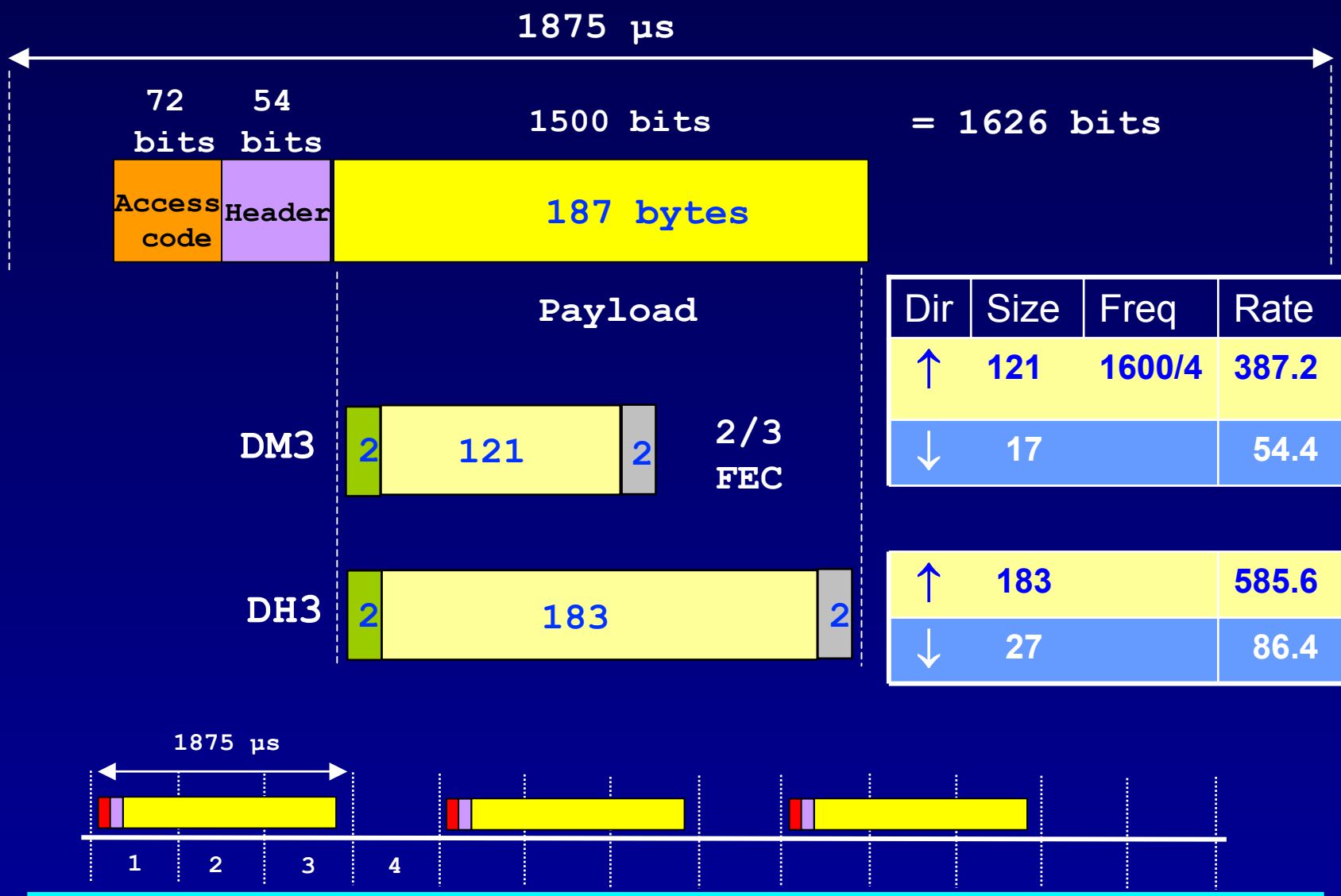
Data rate calculation: DM1 and DH1



Dir	Size	Freq	Rate
↑	17	1600/2	108.8
↓	17		108.8

↑	27	172.8
↓	27	172.8

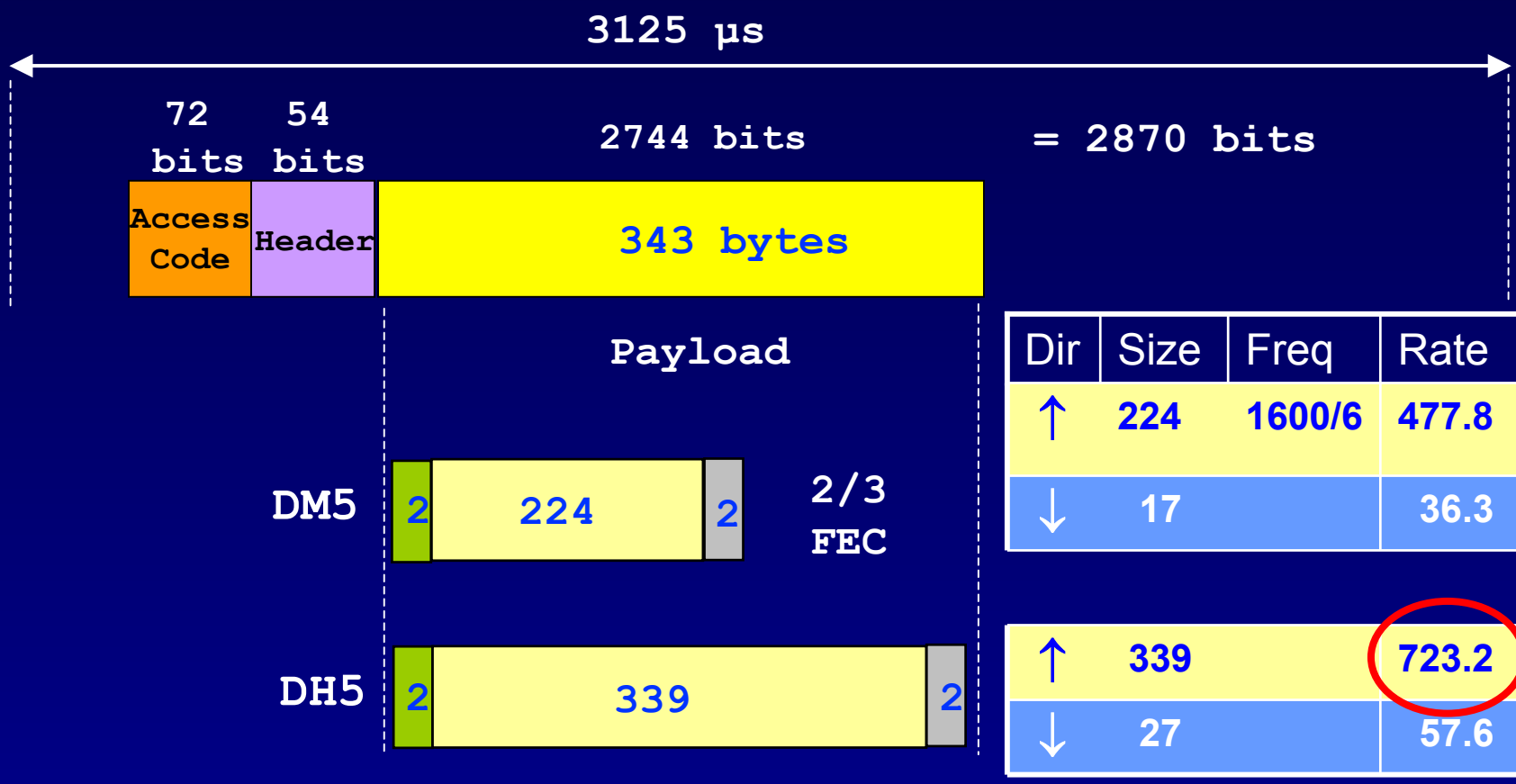
Data rate calculation: DM3 and DH3



Dir	Size	Freq	Rate
↑	121	1600/4	387.2
↓	17		54.4

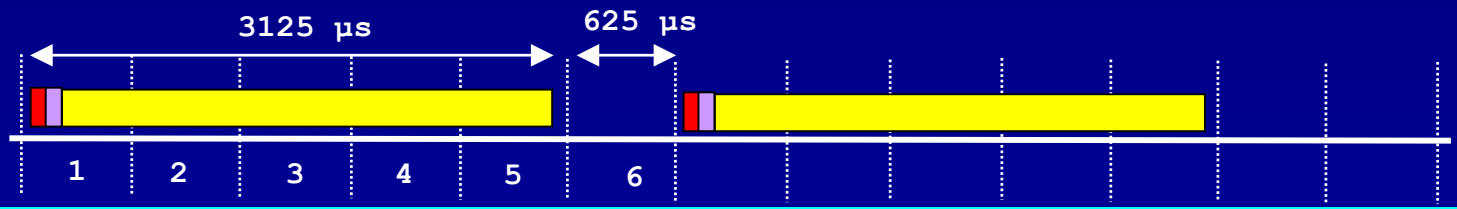
↑	183	585.6
↓	27	86.4

Data rate calculation: DM5 and DH5

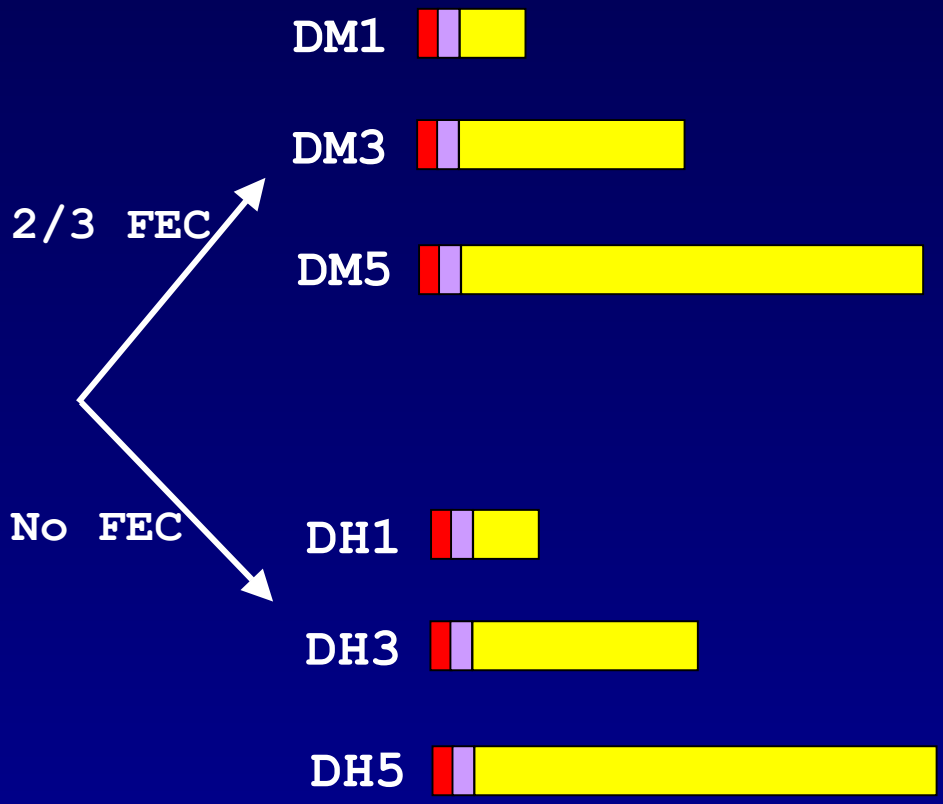


Dir	Size	Freq	Rate
↑	224	1600/6	477.8
↓	17		36.3

↑	339	723.2
↓	27	57.6



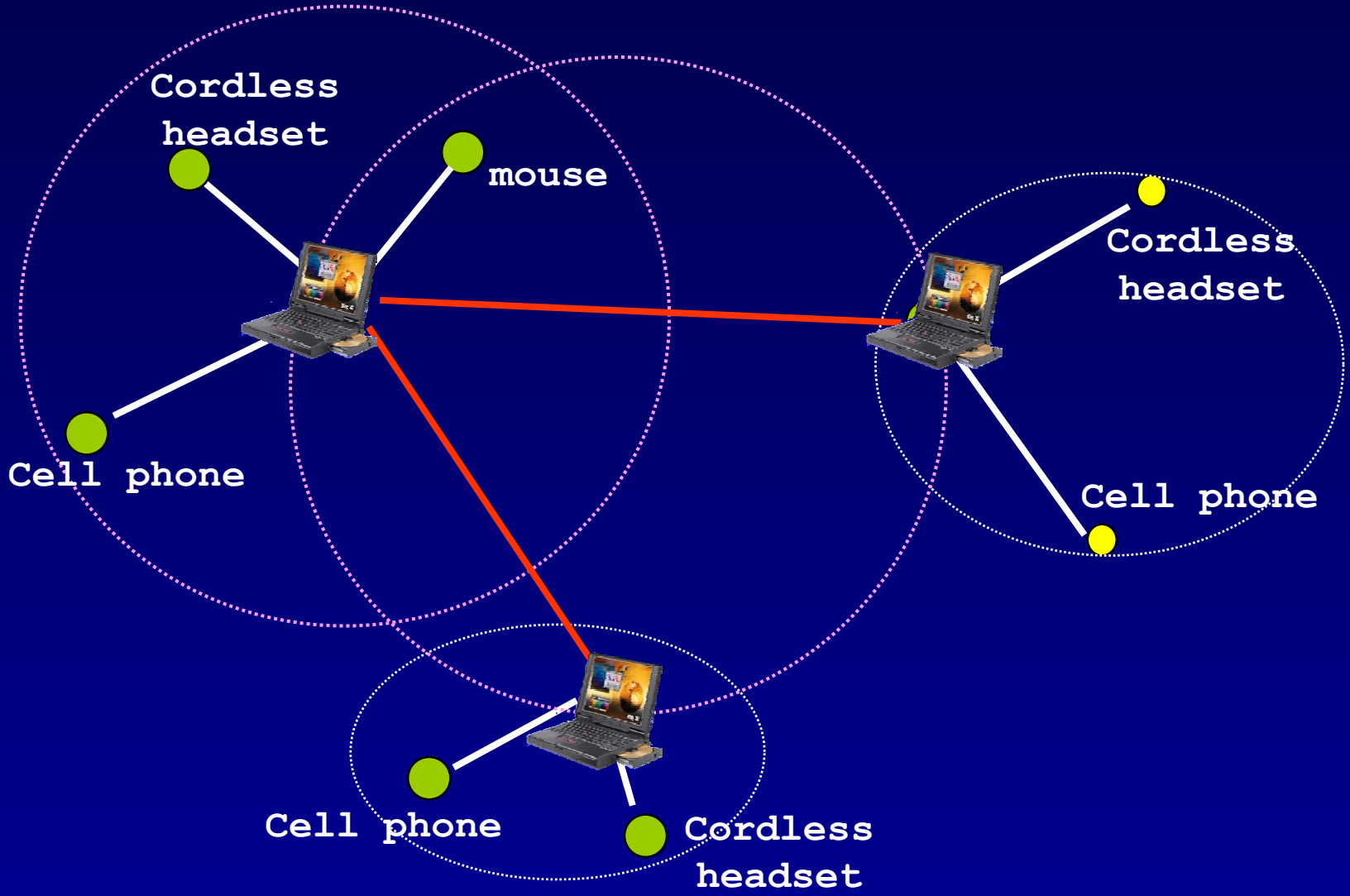
Data Packet Types



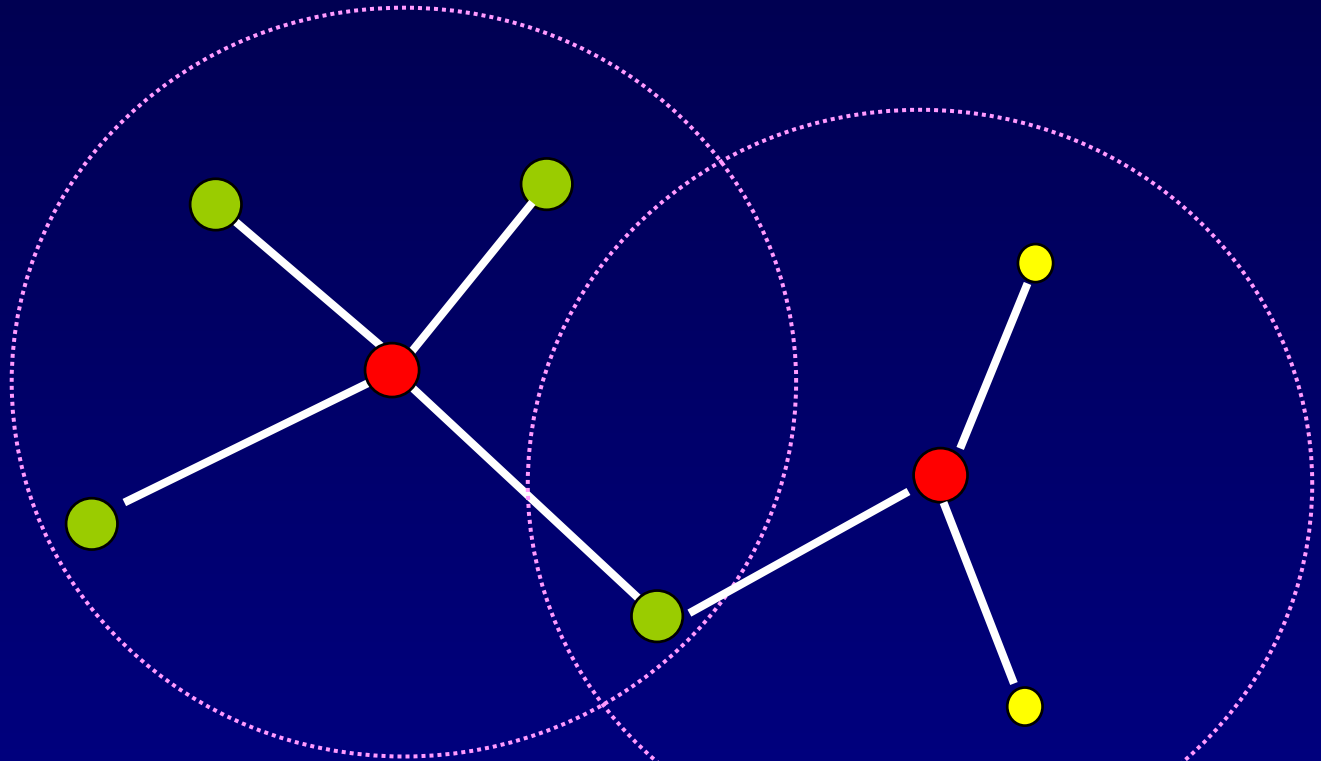
Symmetric	Asymmetric	
108.8	108.8	108.8
258.1	387.2	54.4
286.7	477.8	36.3

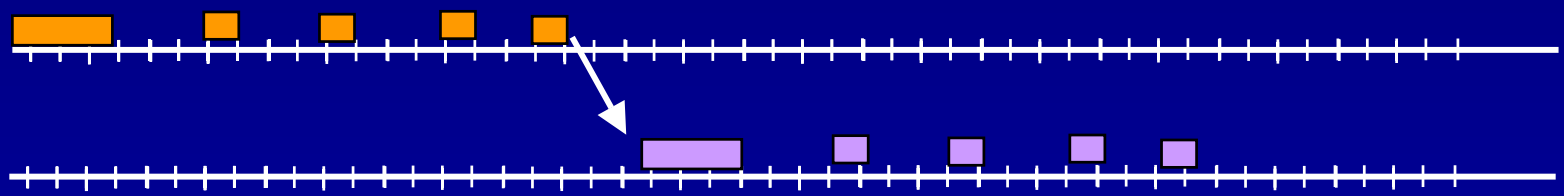
Symmetric	Asymmetric	
172.8	172.8	172.8
390.4	585.6	86.4
433.9	723.2	57.6

Inter piconet communication

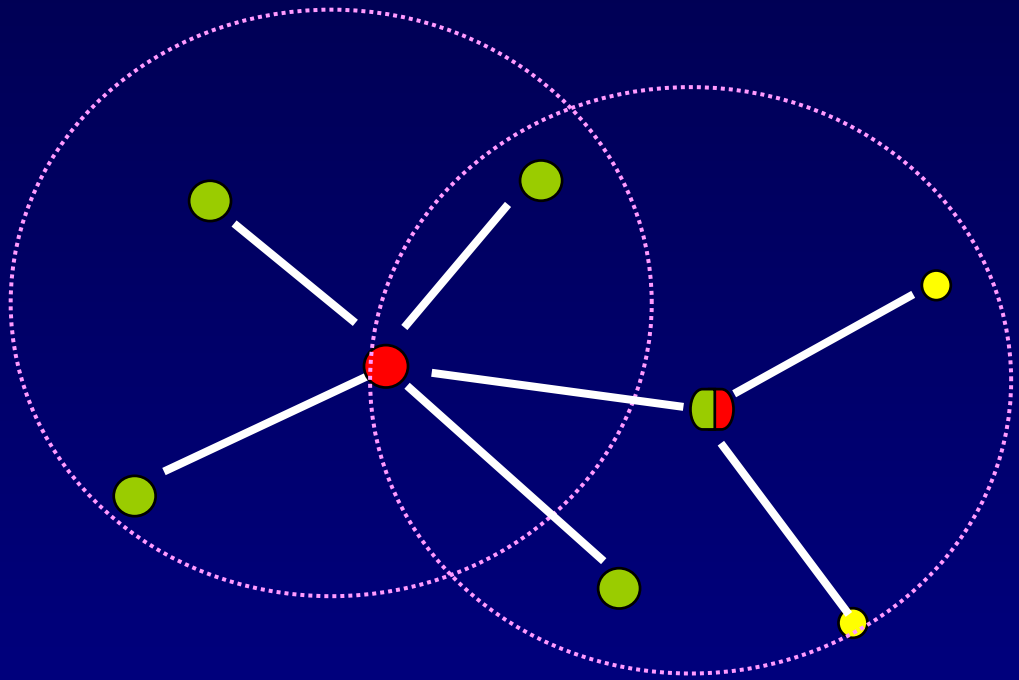


Scatternet





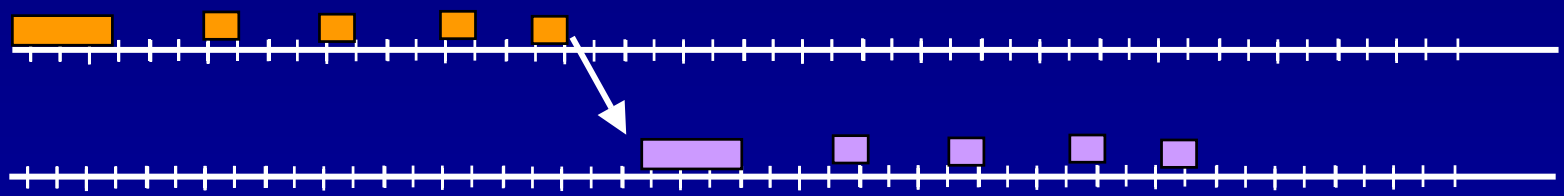
Scatternet, scenario 2



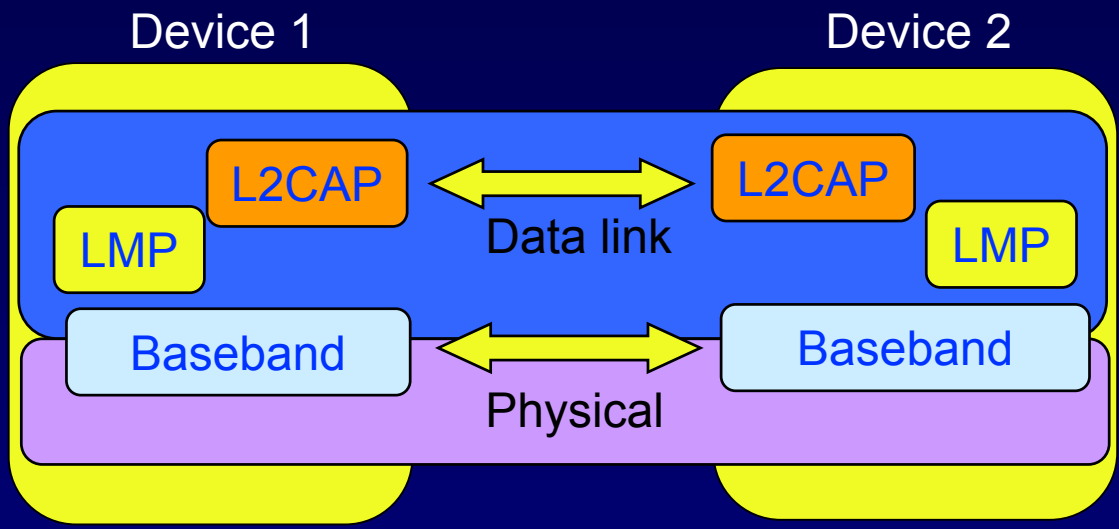
How to schedule presence in two piconets?

Forwarding delay ?

Missed traffic?

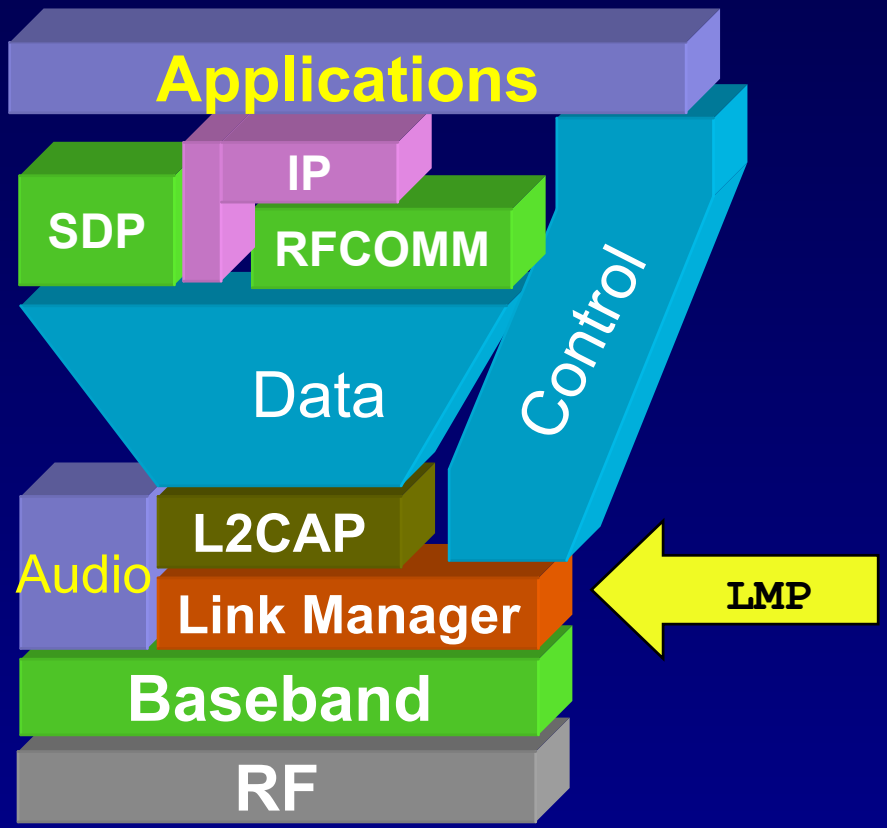


Baseband: Summary



- TDD, frequency hopping physical layer
- Device inquiry and paging
- Two types of links SCO and ACL links
- Multiple packet types (multiple data rates with and without FEC)

Link Manager Protocol

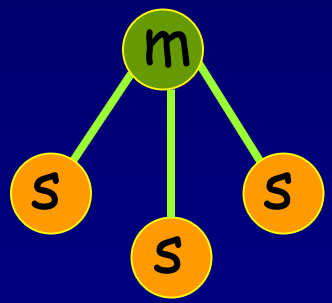


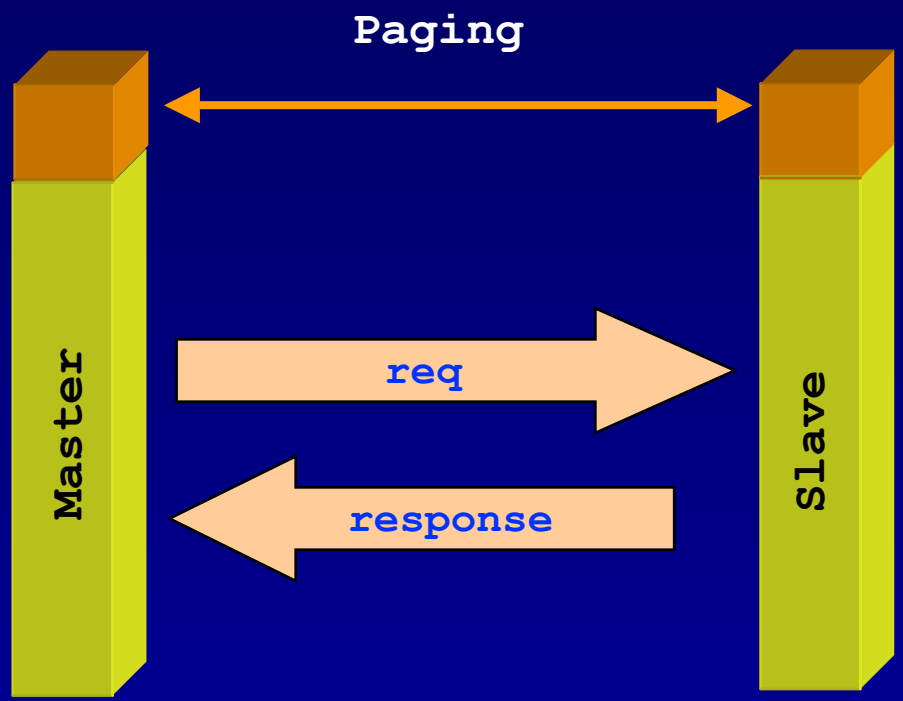
Setup and management of Baseband connections

- Piconet Management
- Link Configuration
- Security

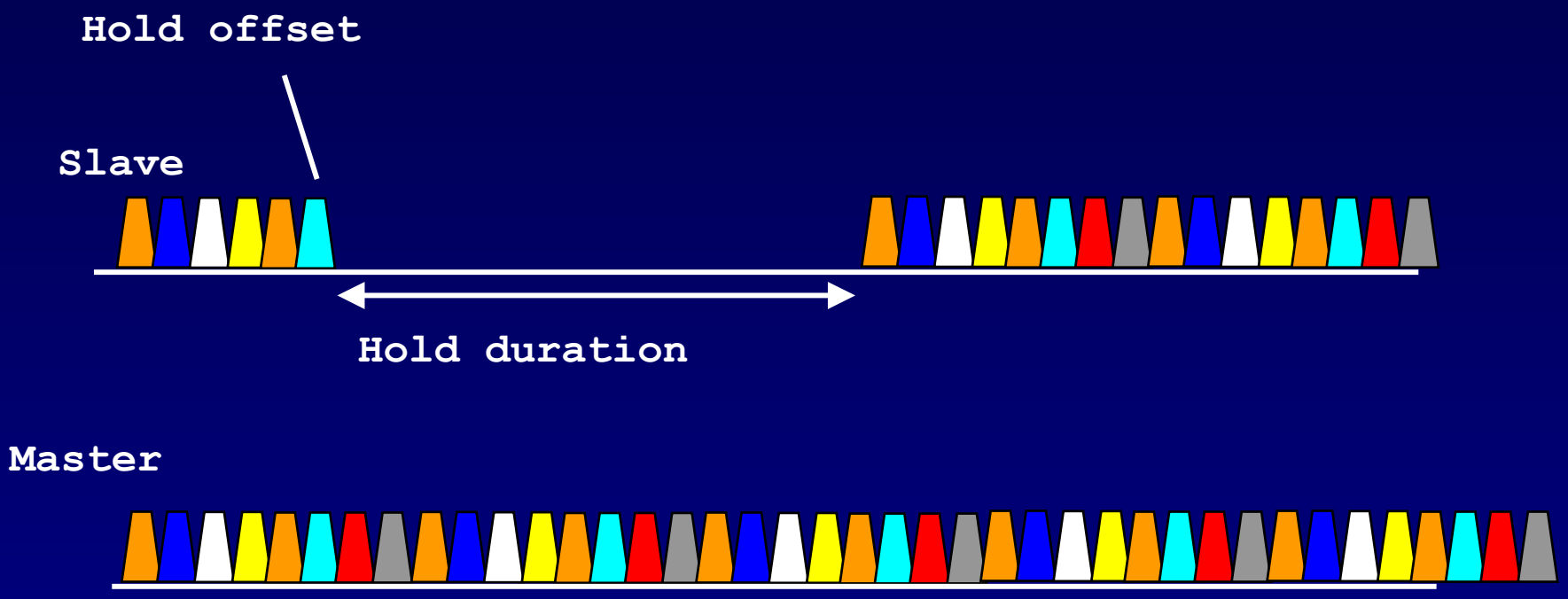
Piconet Management

- Attach and detach slaves
- Master-slave switch
- Establishing SCO links
- Handling of low power modes (Sniff, Hold, Park)

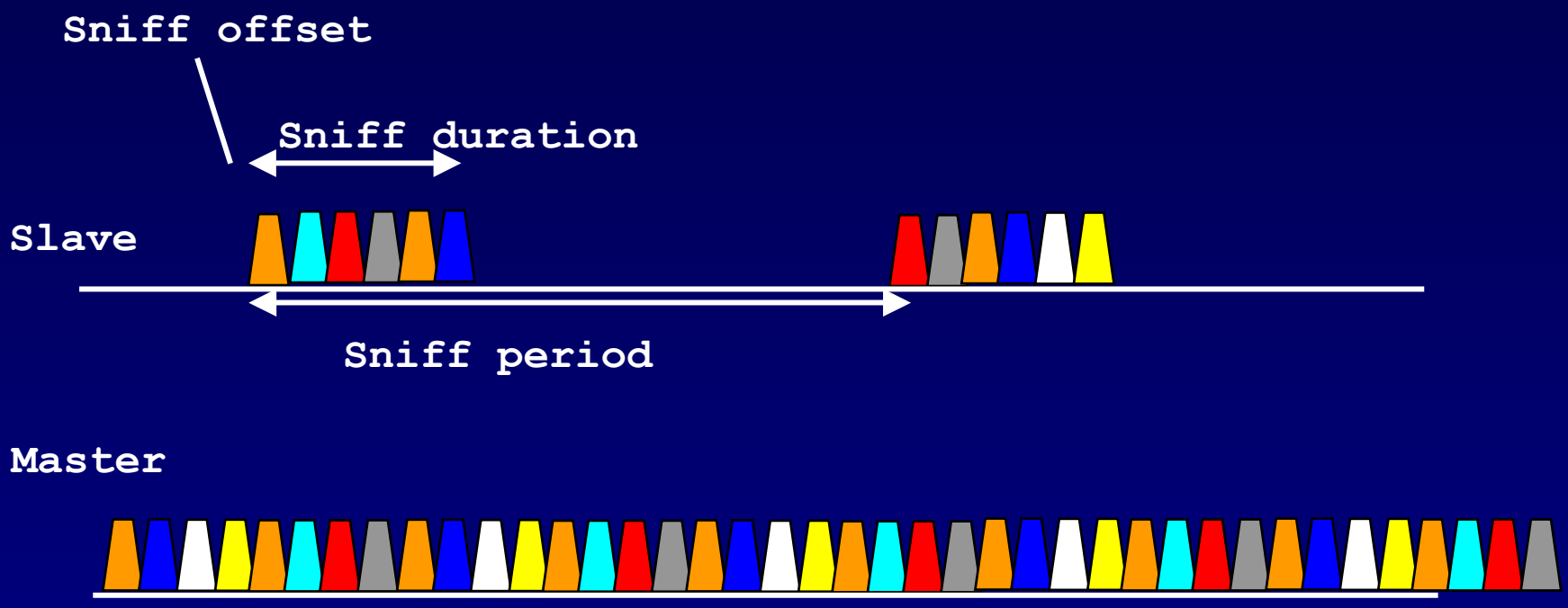




Low power mode (hold)

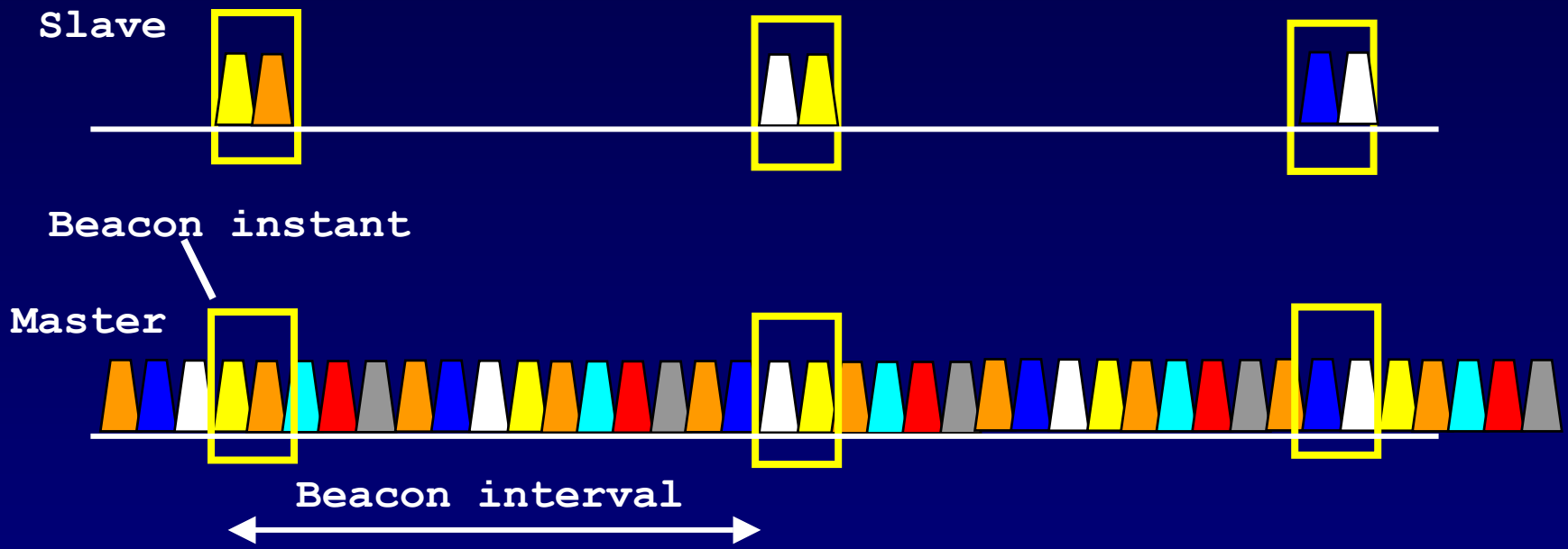


Low power mode (Sniff)



- Traffic reduced to periodic sniff slots

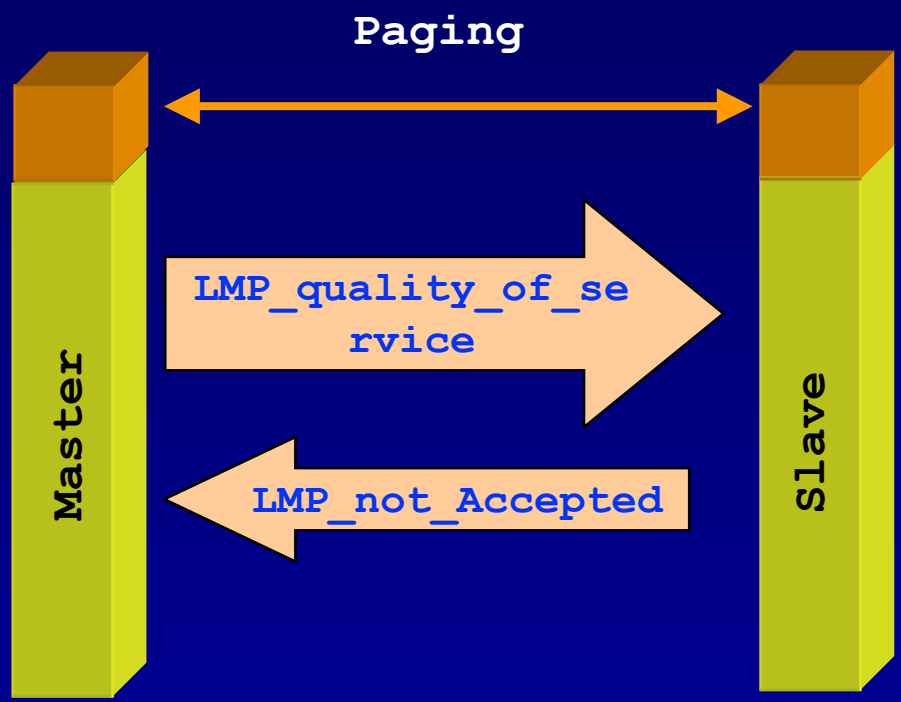
Low power mode (Park)



- Power saving + keep more than 7 slaves in a piconet
- Give up active member address, yet maintain synchronization
- Communication via broadcast LMP messages

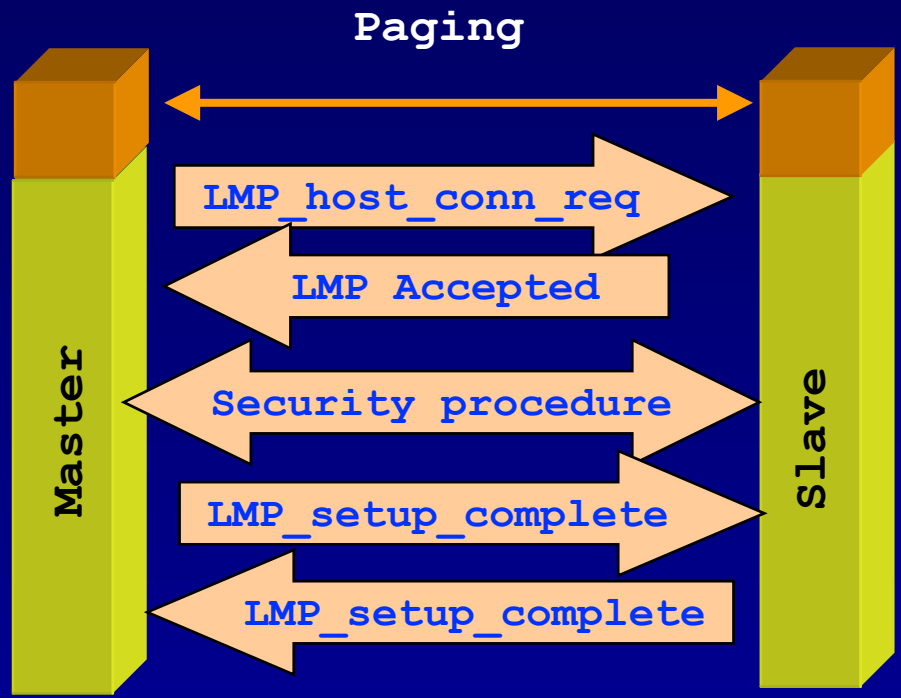
Link Configuration

- Quality of service
  - Polling interval
  - Broadcast repetition
- Power control
- Packet type negotiation
- Multi-slot packets



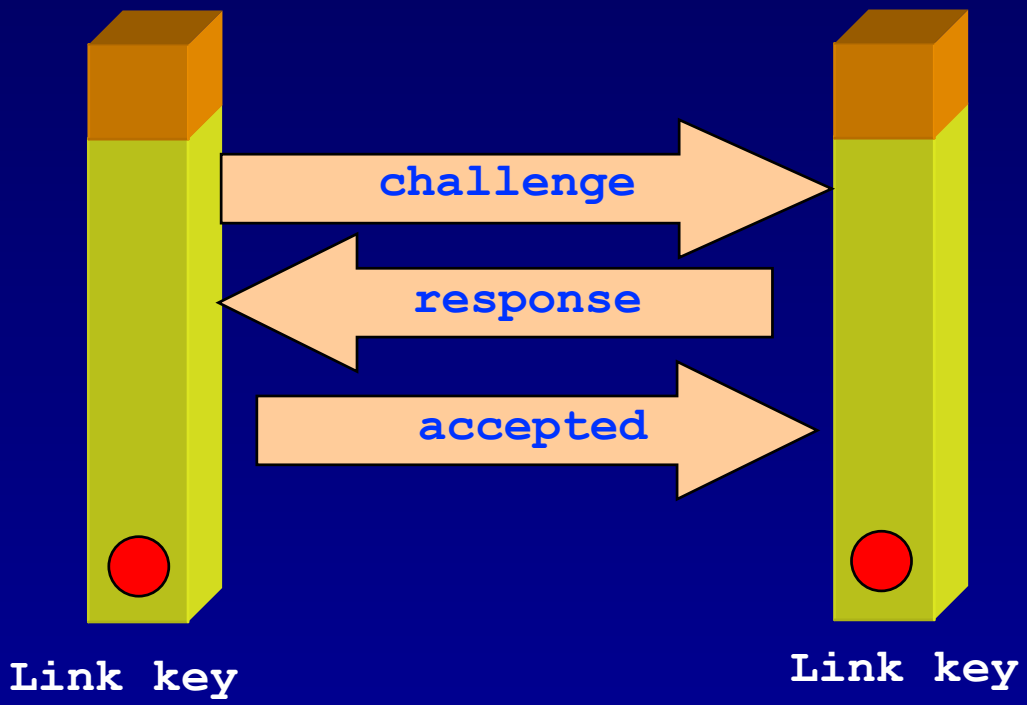
Connection establishment & Security

- Goals
  - Authenticated access
    - Only accept connections from trusted devices
  - Privacy of communication
    - prevent eavesdropping
- Constraints
  - Processing and memory limitations
    - $10 headsets, joysticks
  - Cannot rely on PKI
  - Simple user experience



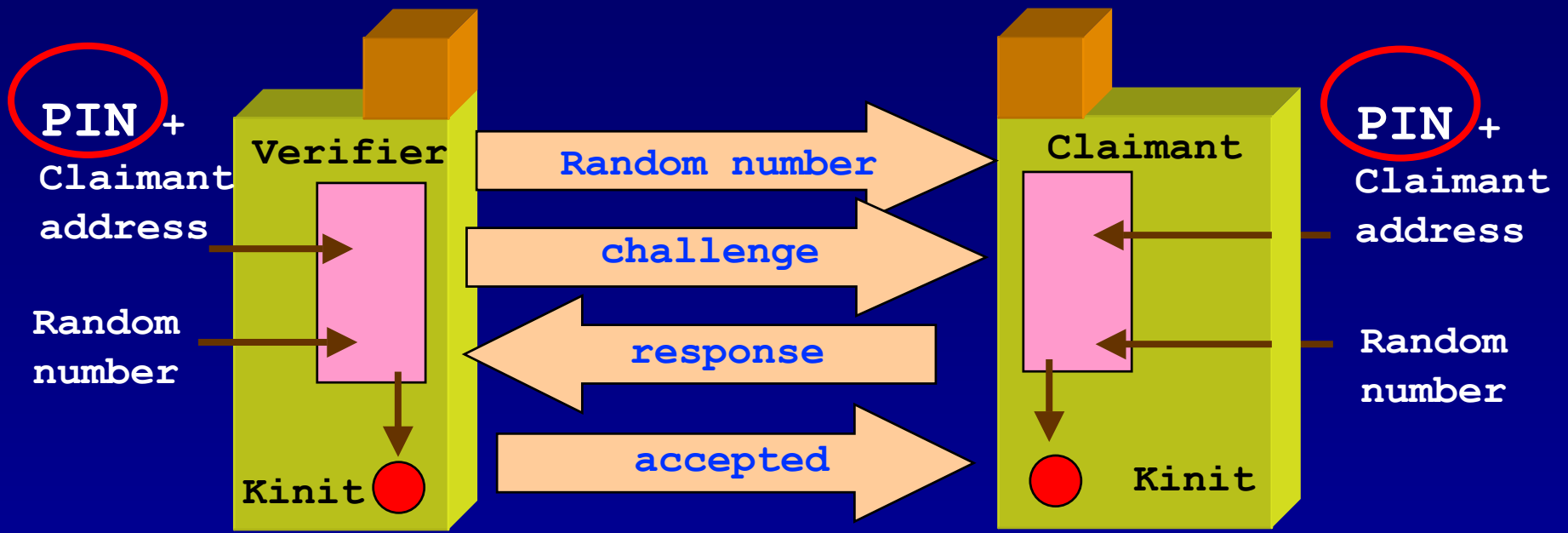
Authentication

- Authentication is based on link key (128 bit shared secret between two devices)
- How can link keys be distributed securely ?



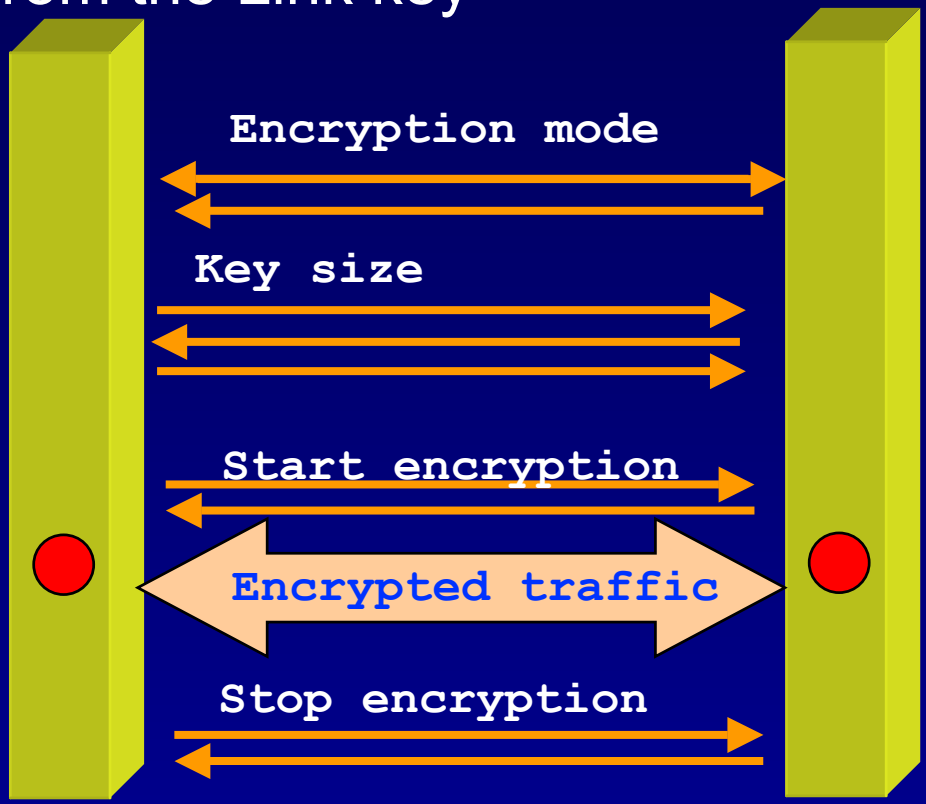
Pairing (key distribution)

- Pairing is a process of establishing a trusted secret channel between two devices (construction of initialization key K_{init})
- K_{init} is then used to distribute unit keys or combination keys

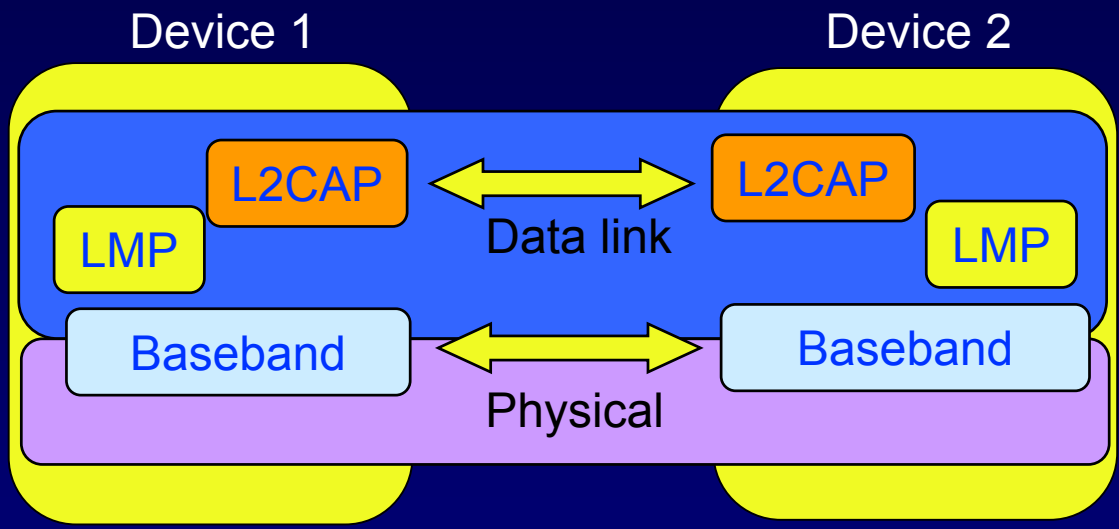


Encryption

- Encryption Key (8 – 128 bits)
- Derived from the Link key

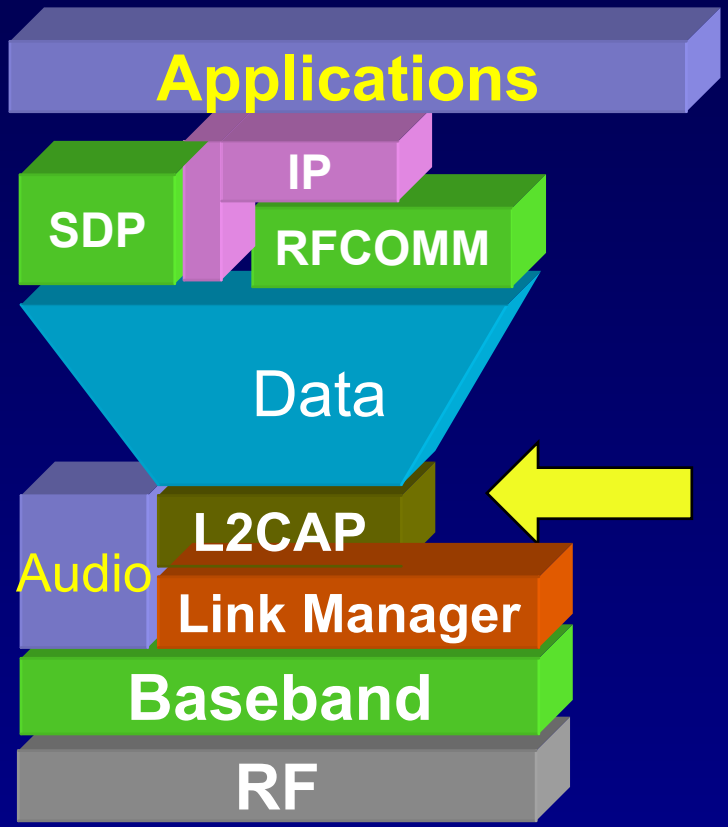


Link Manager Protocol Summary



- Piconet management
- Link configuration
  - Low power modes
  - QoS
  - Packet type selection
- Security: authentication and encryption

L2CAP

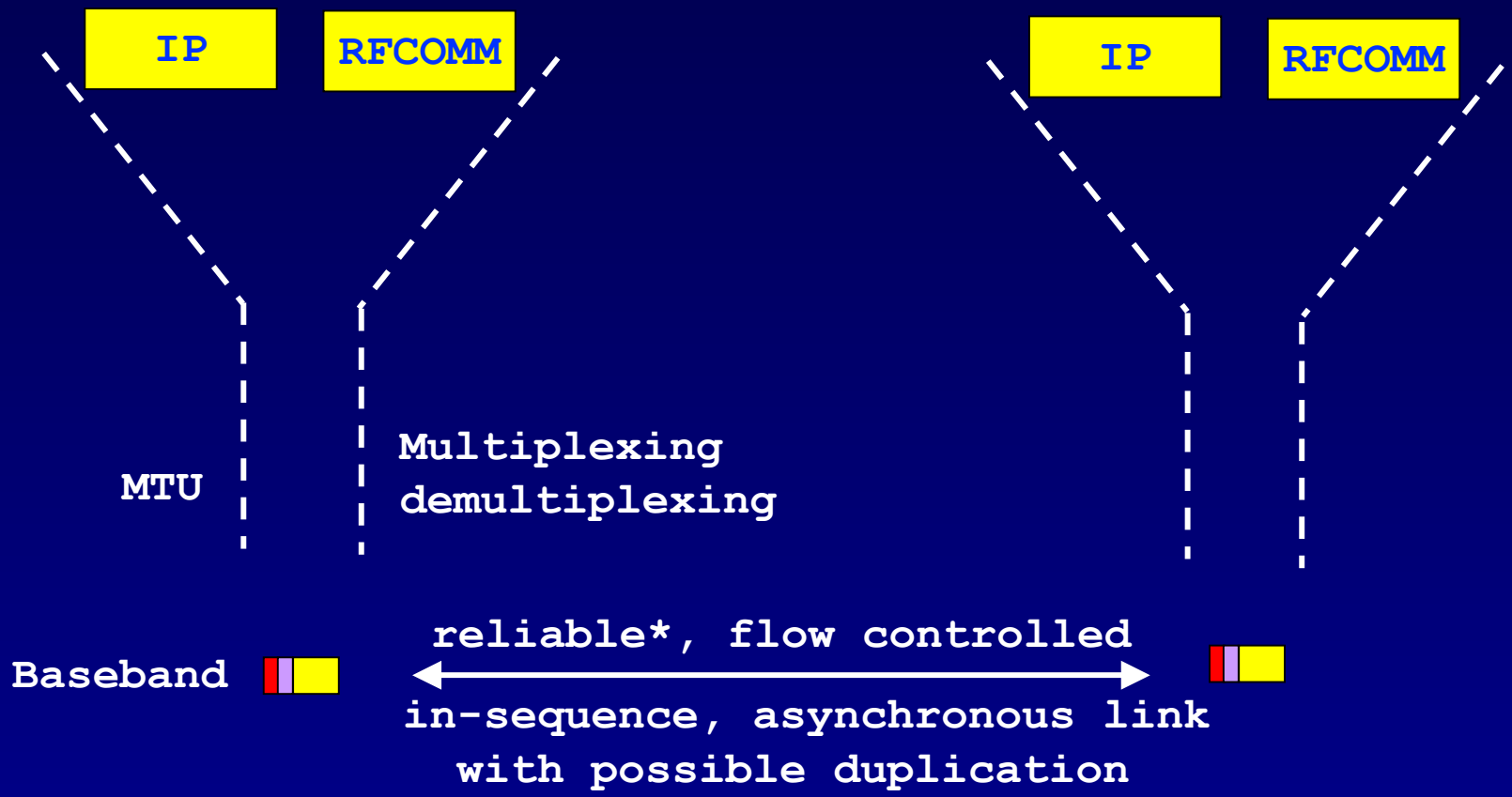


Logical Link Control and Adaptation Protocol

L2CAP provides

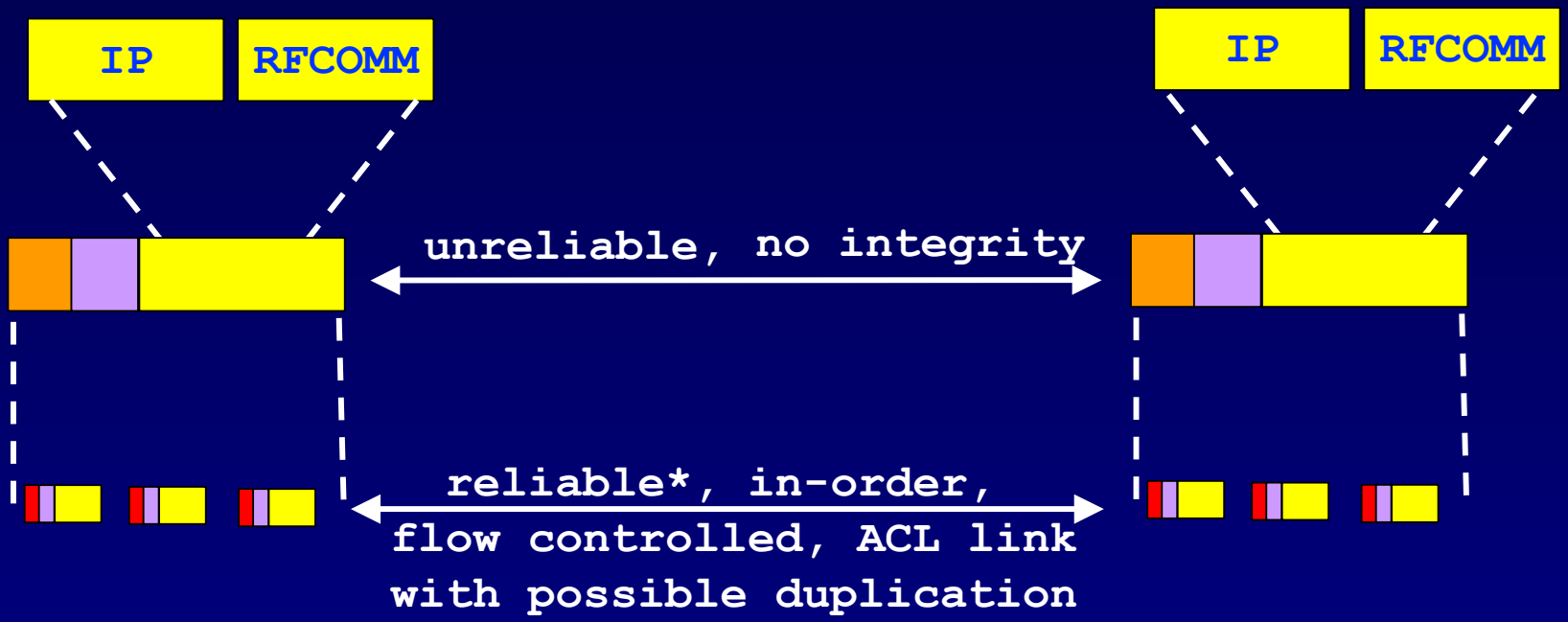
- Protocol multiplexing
- Segmentation and Re-assembly
- Quality of service negotiation

Why baseband isn't sufficient



- Baseband packet size is very small (17min, 339 max)
- No protocol-id field in the baseband header

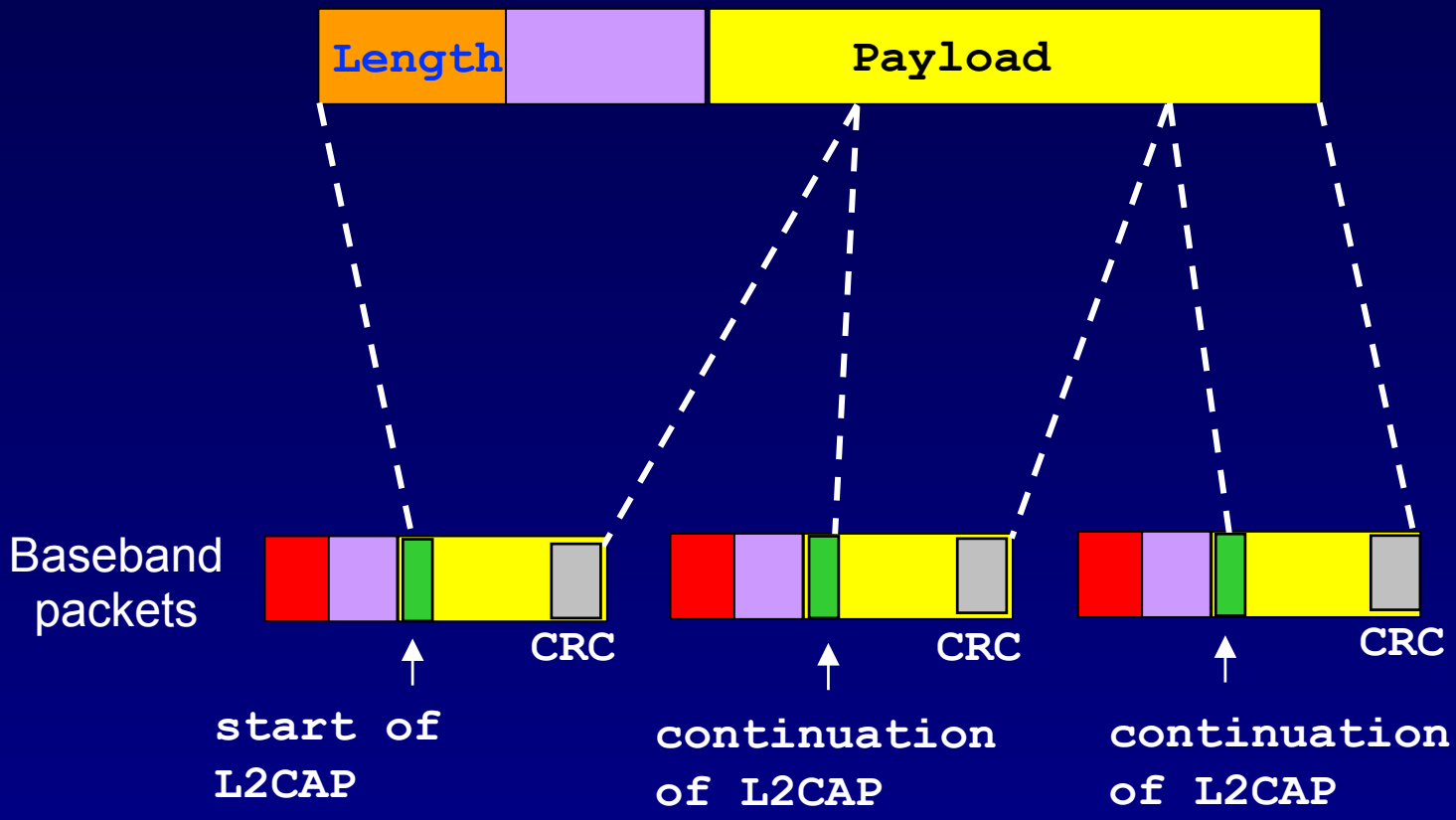
Need a multiprotocol encapsulation layer



Desired features
- Protocol multiplexing
- Segmentation and re-assembly
- Quality of service

What about
- Reliability?
- Connection oriented or connectionless?
- integrity checks?

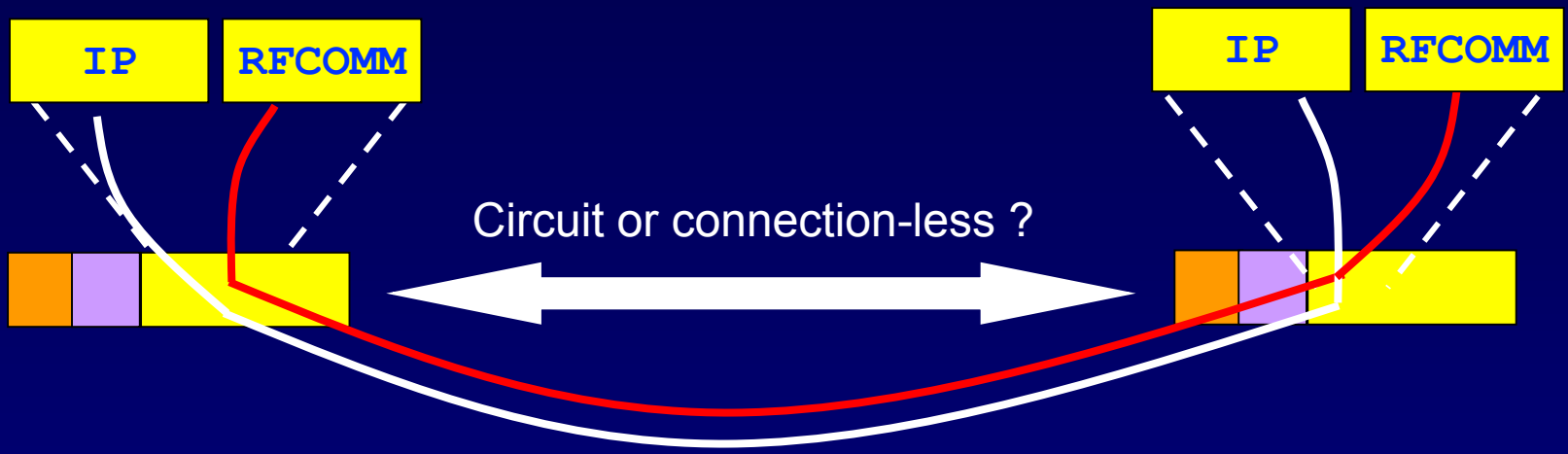
Segmentation and reassembly



- cannot cope with re-ordering or loss
- mixing of multiple L2CAP fragments not allowed
- If the start of L2CAP packet is not acked, the rest should be discarded

min MTU = 48
672 default

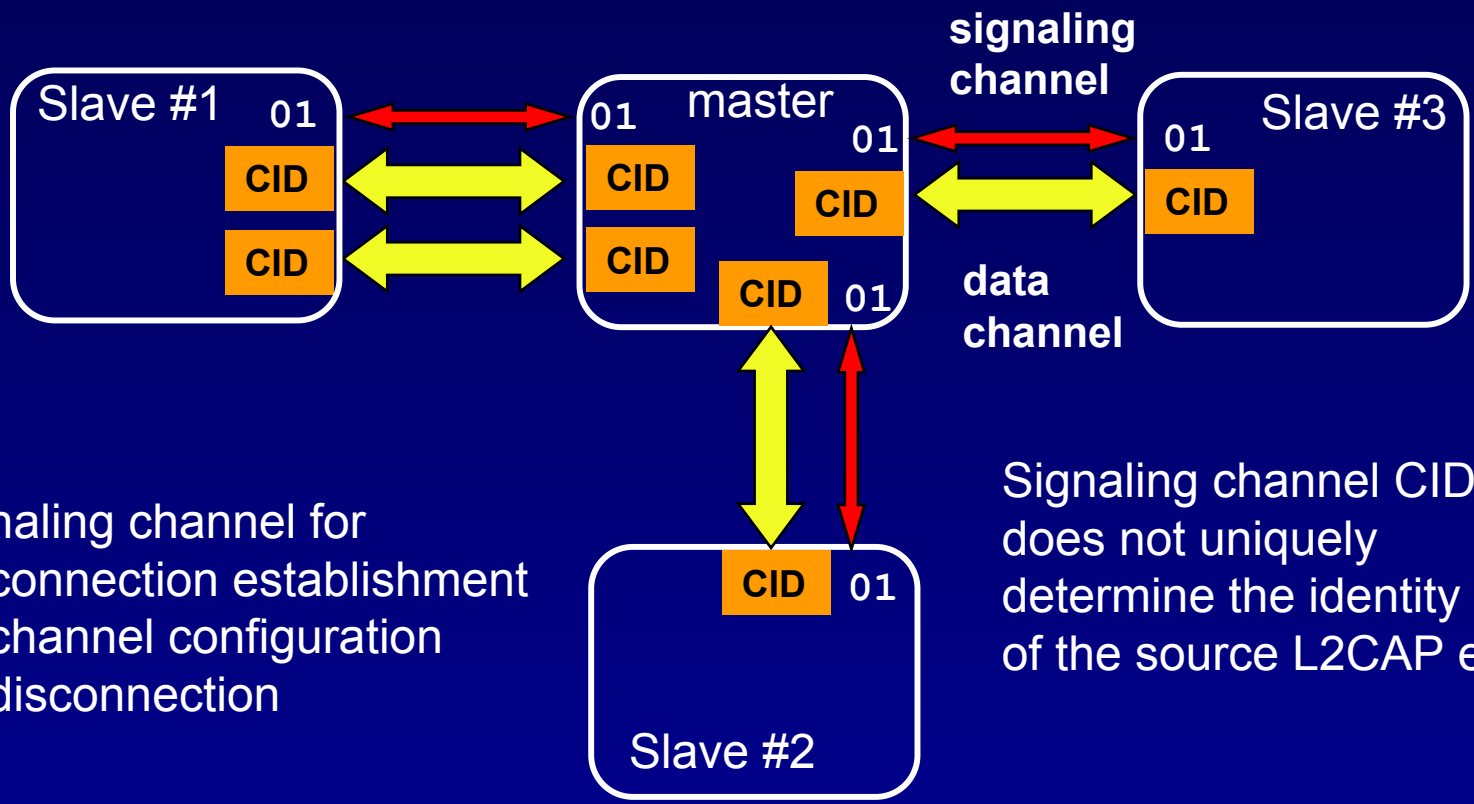
Multiplexing and Demultiplexing



Why is L2CAP connection oriented ?

- Baseband is polling based
- Bandwidth efficiency
  - carry state in each packet Vs. maintain it at end-points
- Need ability for logical link configuration
  - MTU
  - reliability (Flush timeout option)
  - QoS (token bucket parameter negotiation)

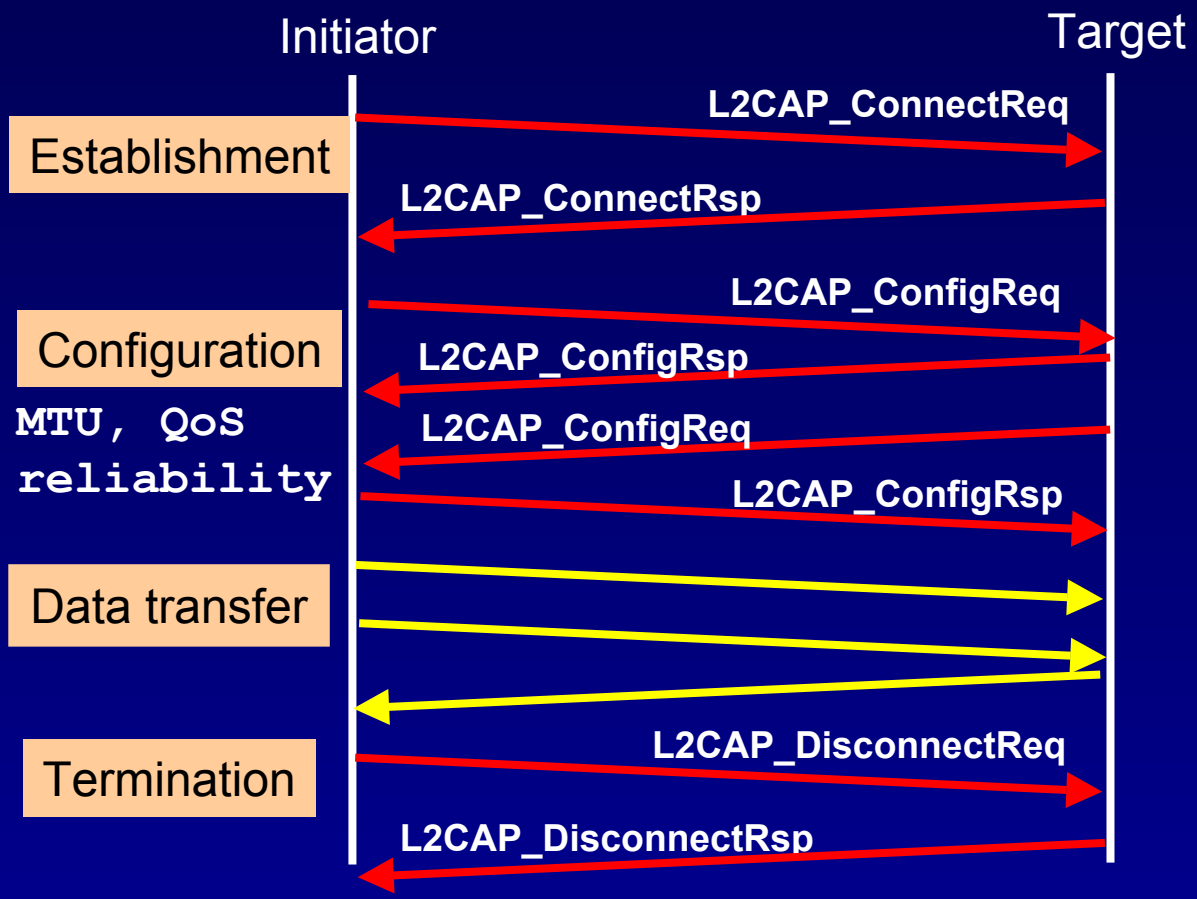
L2CAP Channels



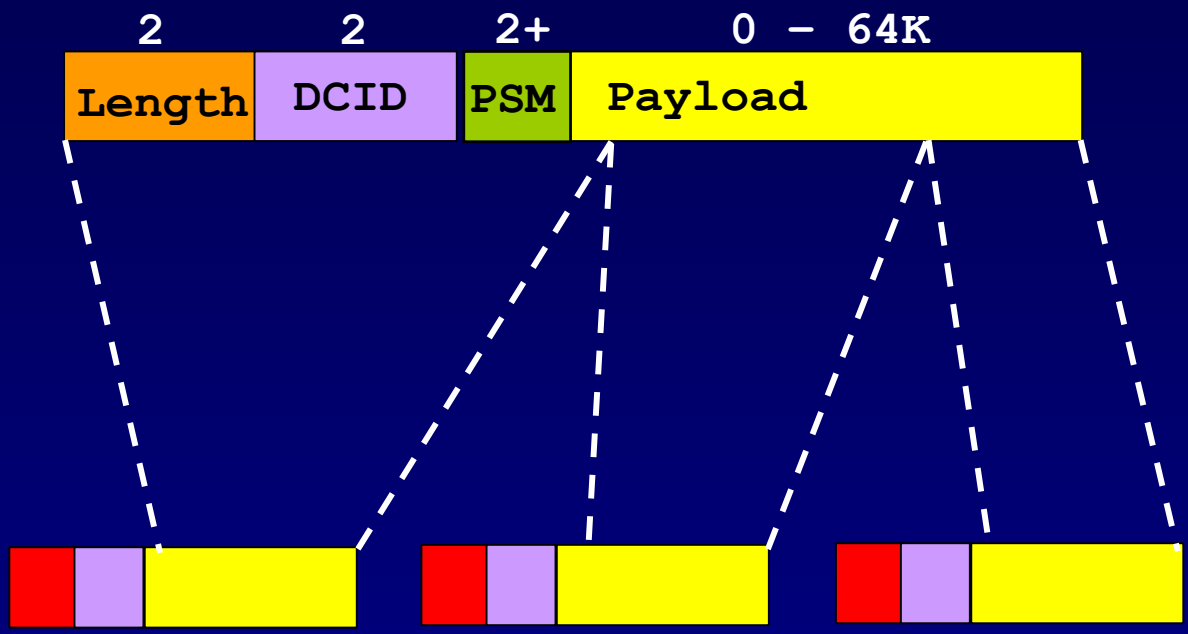
Signaling channel for
1) connection establishment
2) channel configuration
3) disconnection

Signaling channel CID does not uniquely determine the identity of the source L2CAP entity

L2CAP connection: an example



L2CAP Packet Format (Connectionless)



Not fully developed yet.

L2CAP: Summary

Design constraints:

- Simplicity
- Low overhead
- Limited computation and memory
- Power efficient

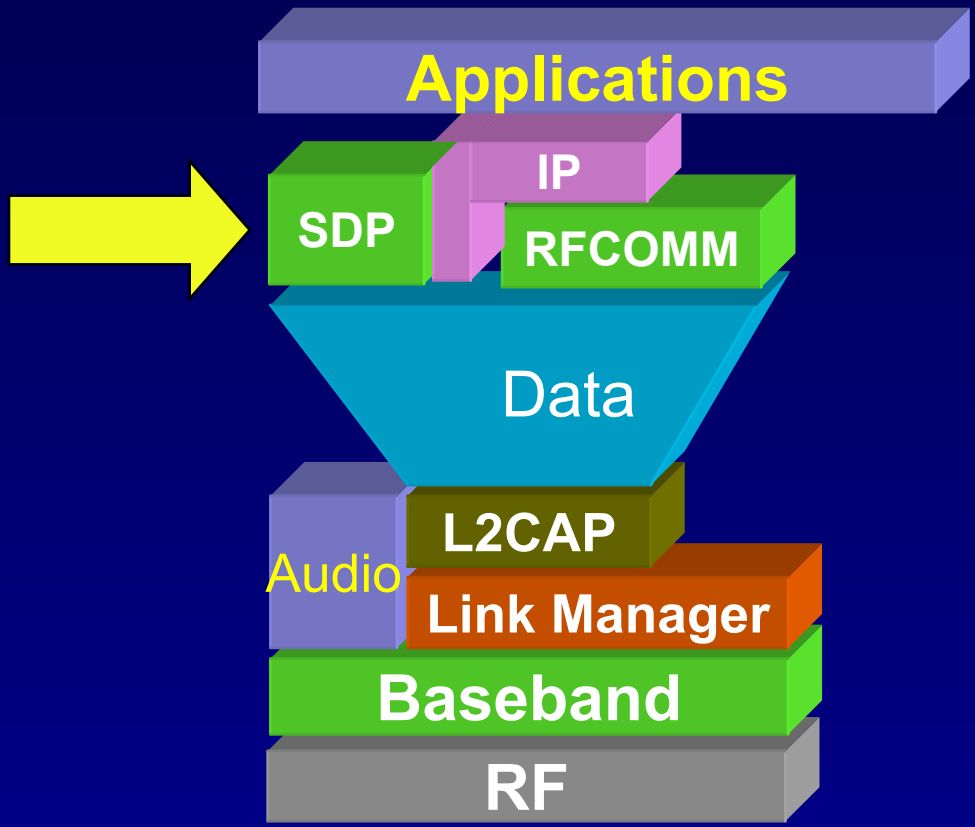
Assumptions about the lower layer

- Reliable, in-order delivery of fragments
- Integrity checks on each fragment
- Asynchronous, best effort point-to-point link
- No duplication
- Full duplex

Service provided to the higher layer

- Protocol multiplexing and demultiplexing
- Larger MTU than baseband
- Point to point communication

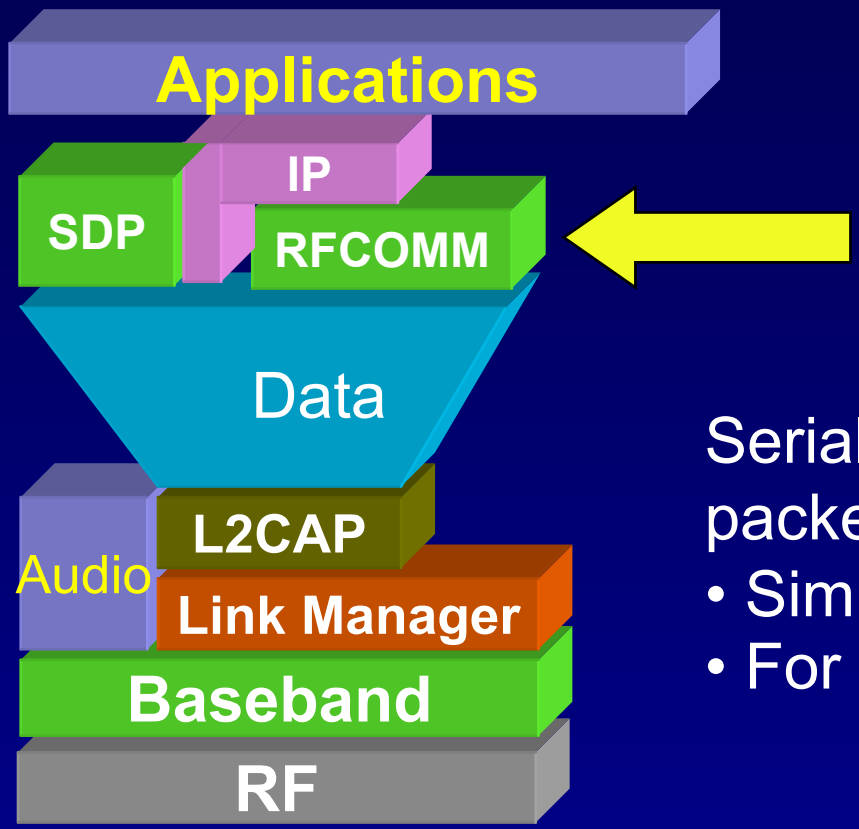
Bluetooth Service Discovery Protocol



Example 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

Serial Port Emulation using RFCOMM



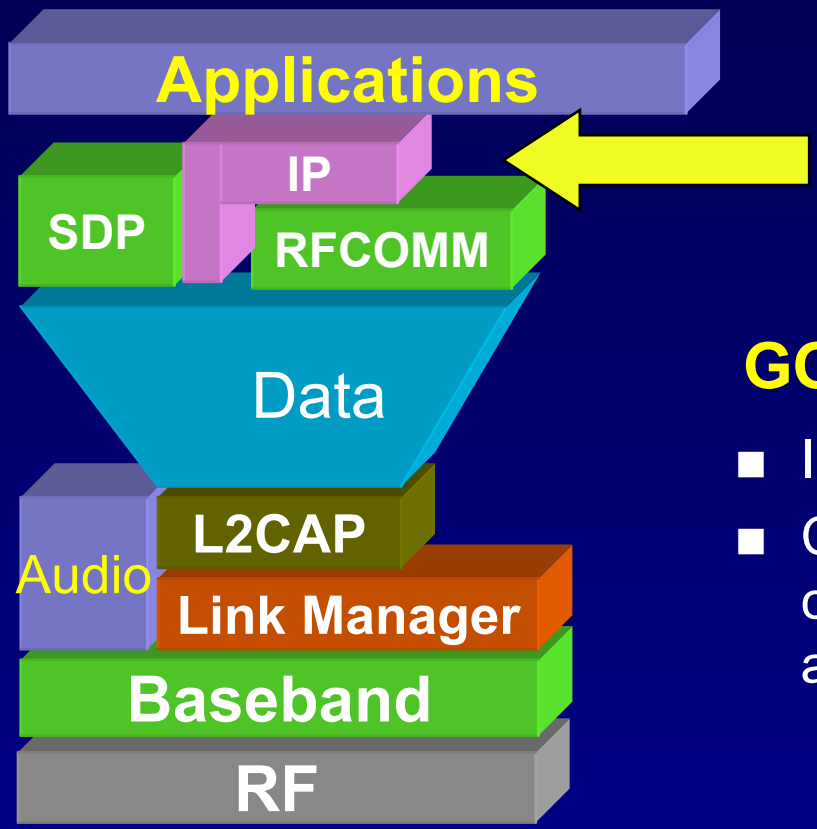
Serial Port emulation on top of a packet oriented link

- Similar to HDLC
- For supporting legacy apps

Serial line emulation over packet based MAC

- Design considerations
  - framing: assemble bit stream into bytes and, subsequently, into packets
  - transport: in-sequence, reliable delivery of serial stream
  - control signals: RTS, CTS, DTR

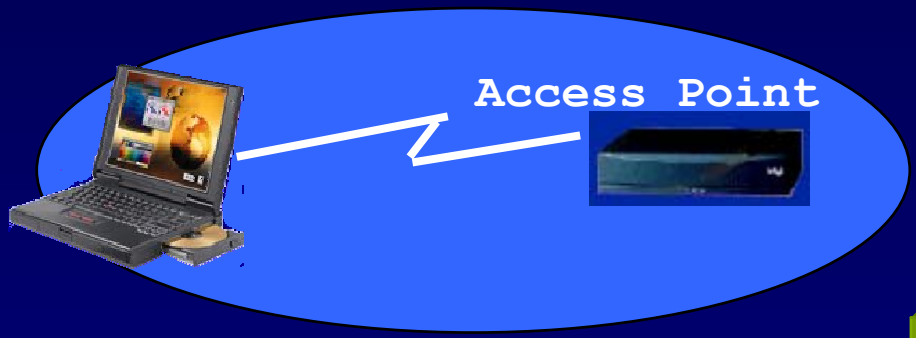
IP over Bluetooth V 1.0



GOALS

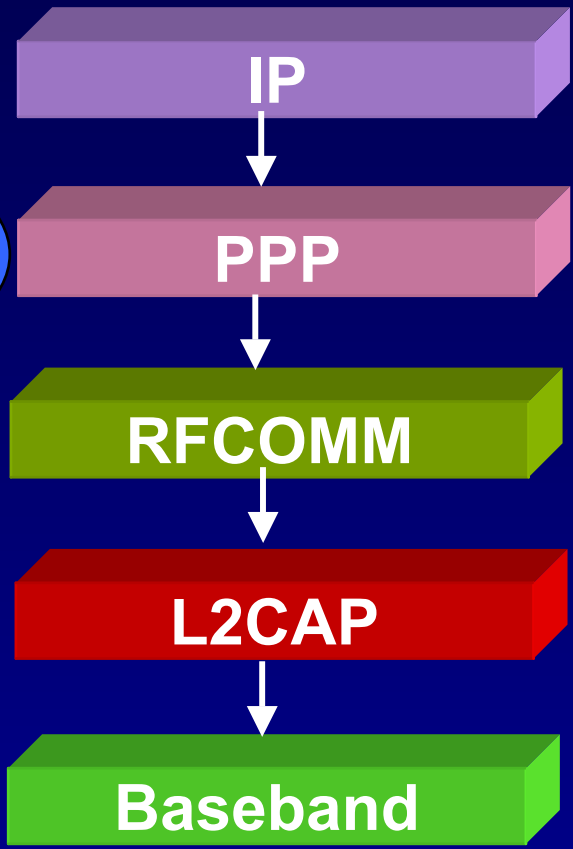
- Internet access using cell phones
- Connect PDA devices & laptop computers to the Internet via LAN access points

LAN access point profile



Why use PPP?

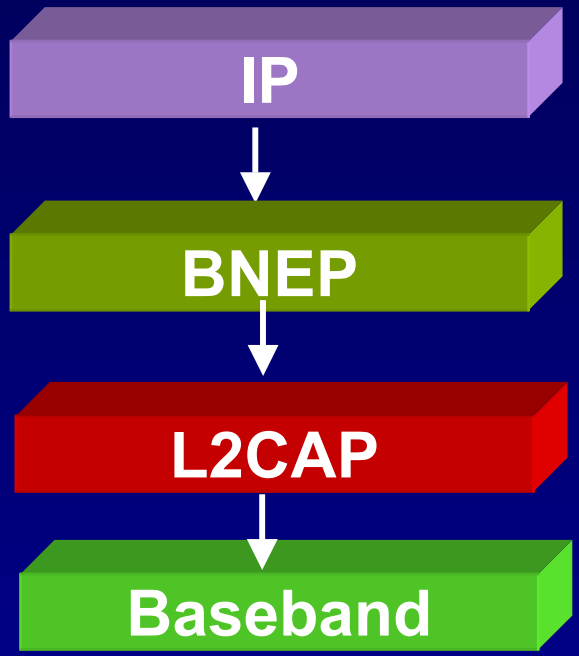
- Security
  - Authentication
  - Access control
- Efficiency
  - header and data compression
- Auto-configuration
- Lower barrier for deployment



IP over Bluetooth v 1.1: BNEP

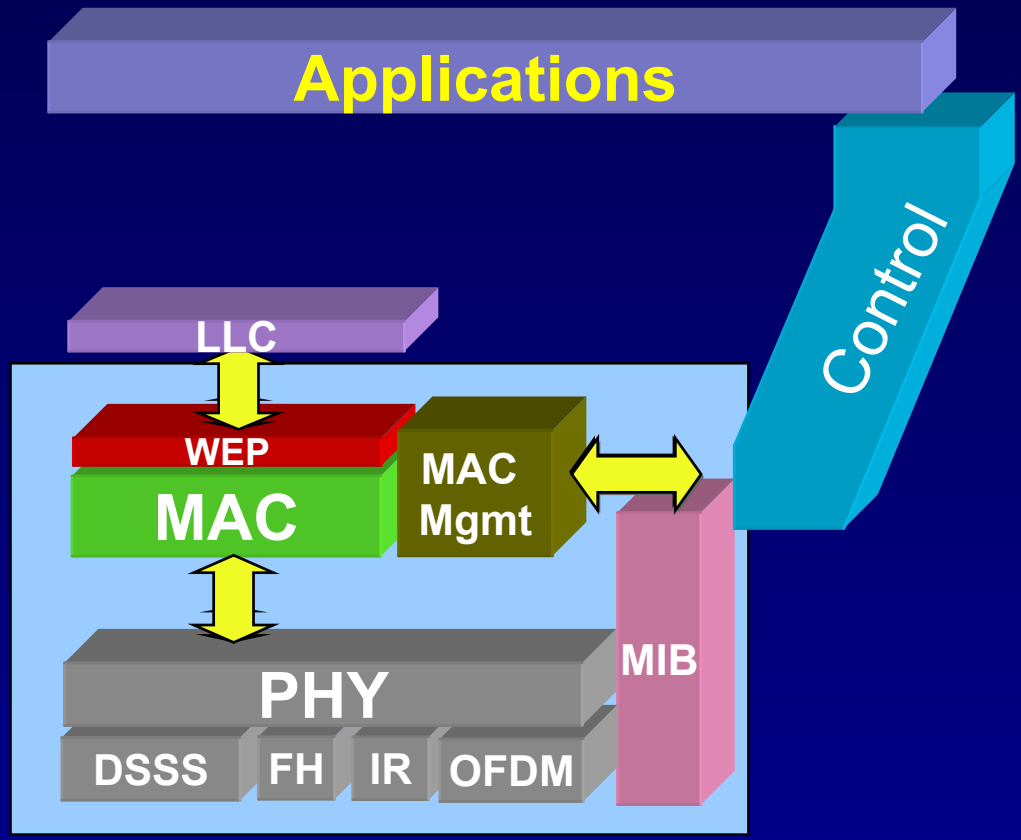
Bluetooth Network Encapsulation Protocol (BNEP) provides emulation of Ethernet over L2CAP

- BNEP defines
  - a frame format which includes IEEE 48 bit MAC addresses
  - A method for encapsulating BNEP frames using L2CAP
- Option to compress header fields to conserve space
- Control messages to activate filtering of messages at Access Point



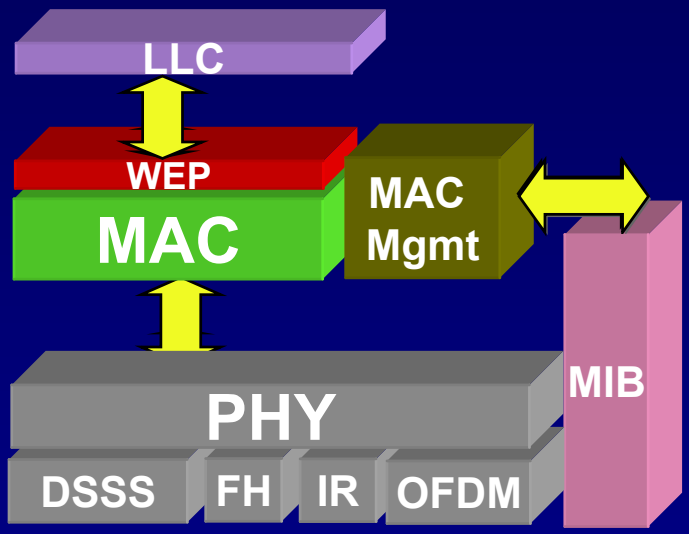
802.11 specifications overview

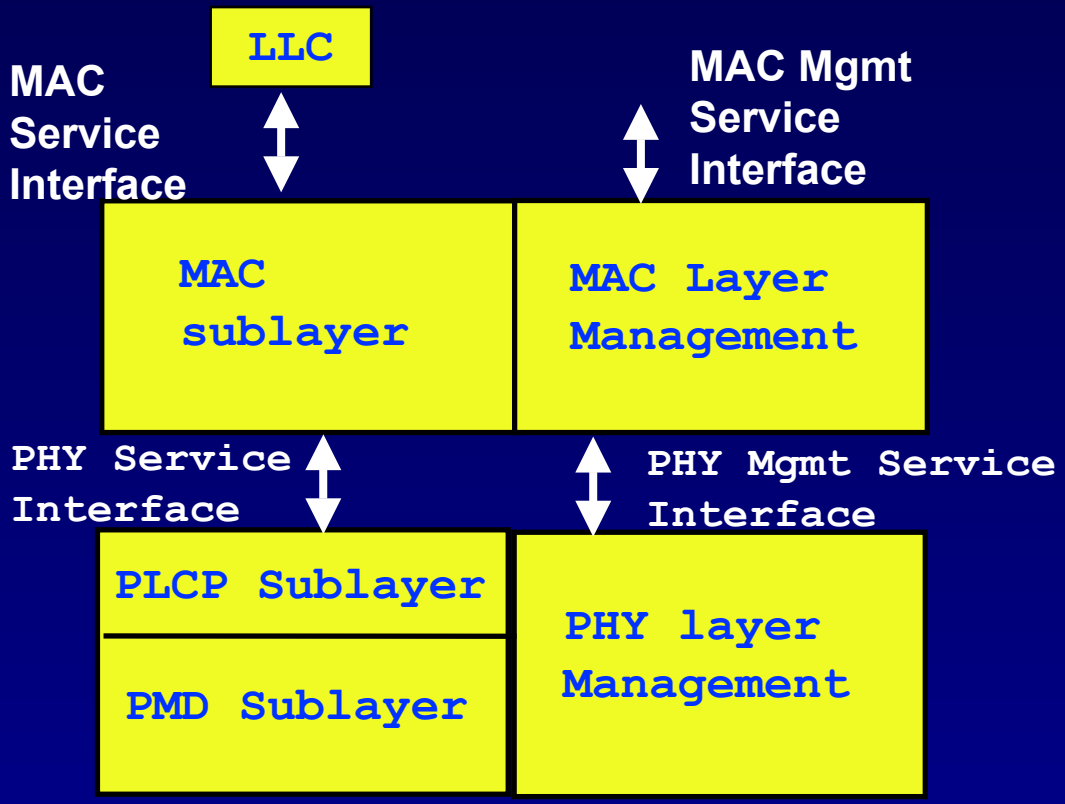
802.11 Specifications



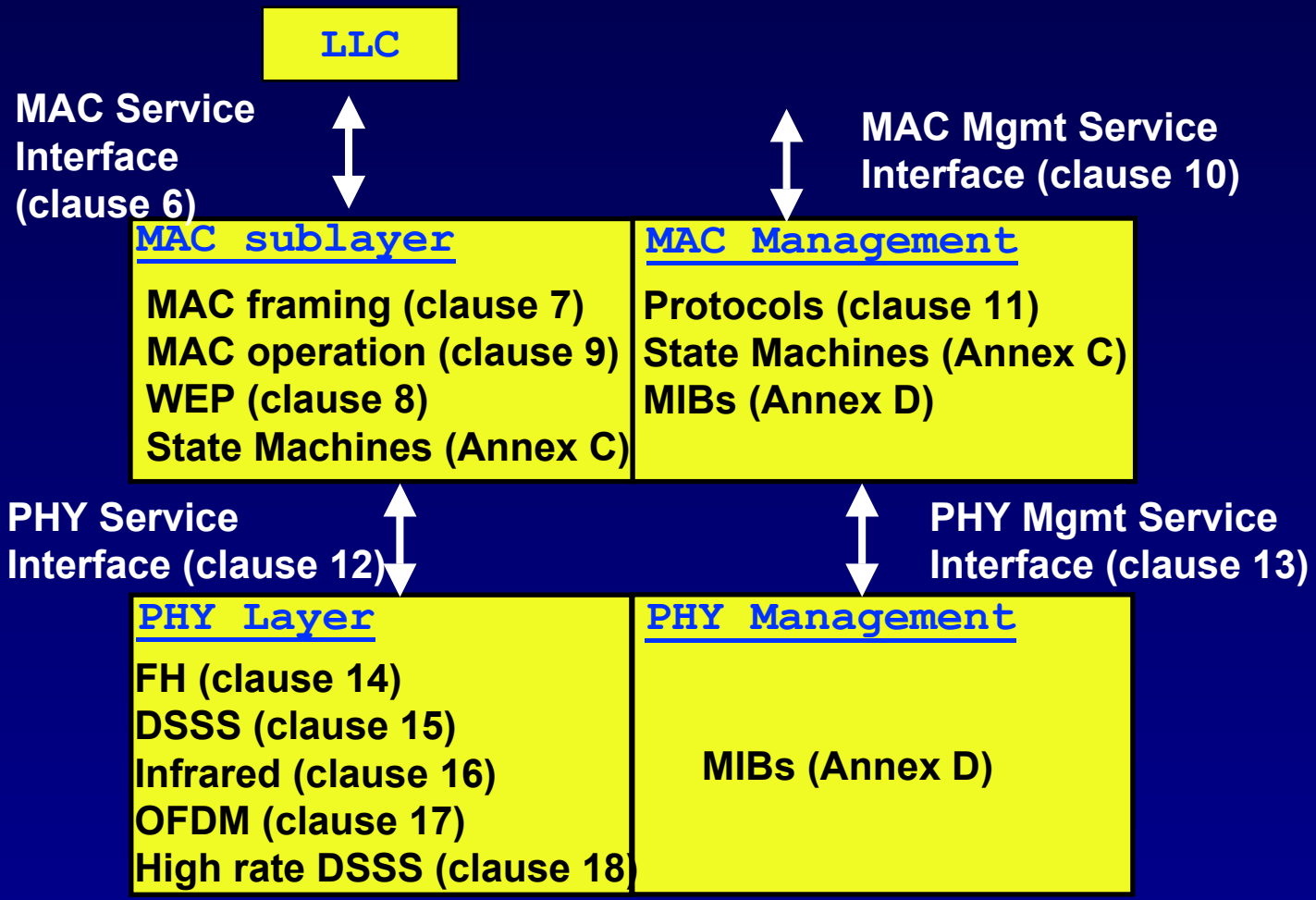
- Specification of layers below LLC
- Associated management/control interfaces

802.11 Specifications





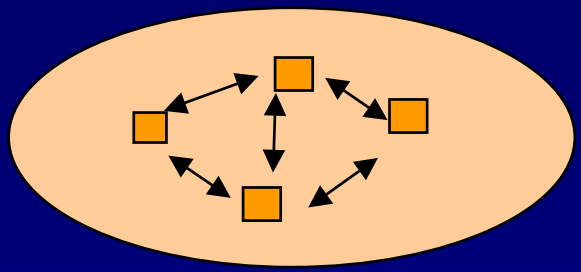
802.11 Specifications



802.11 System Architecture

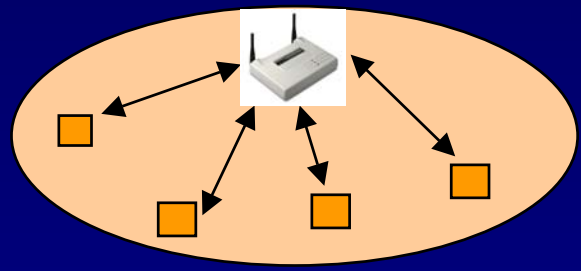
Basic Service Set (BSS): a set of stations which communicate with one another

Independent Basic Service Set (IBSS)



- only direct communication possible
- no relay function

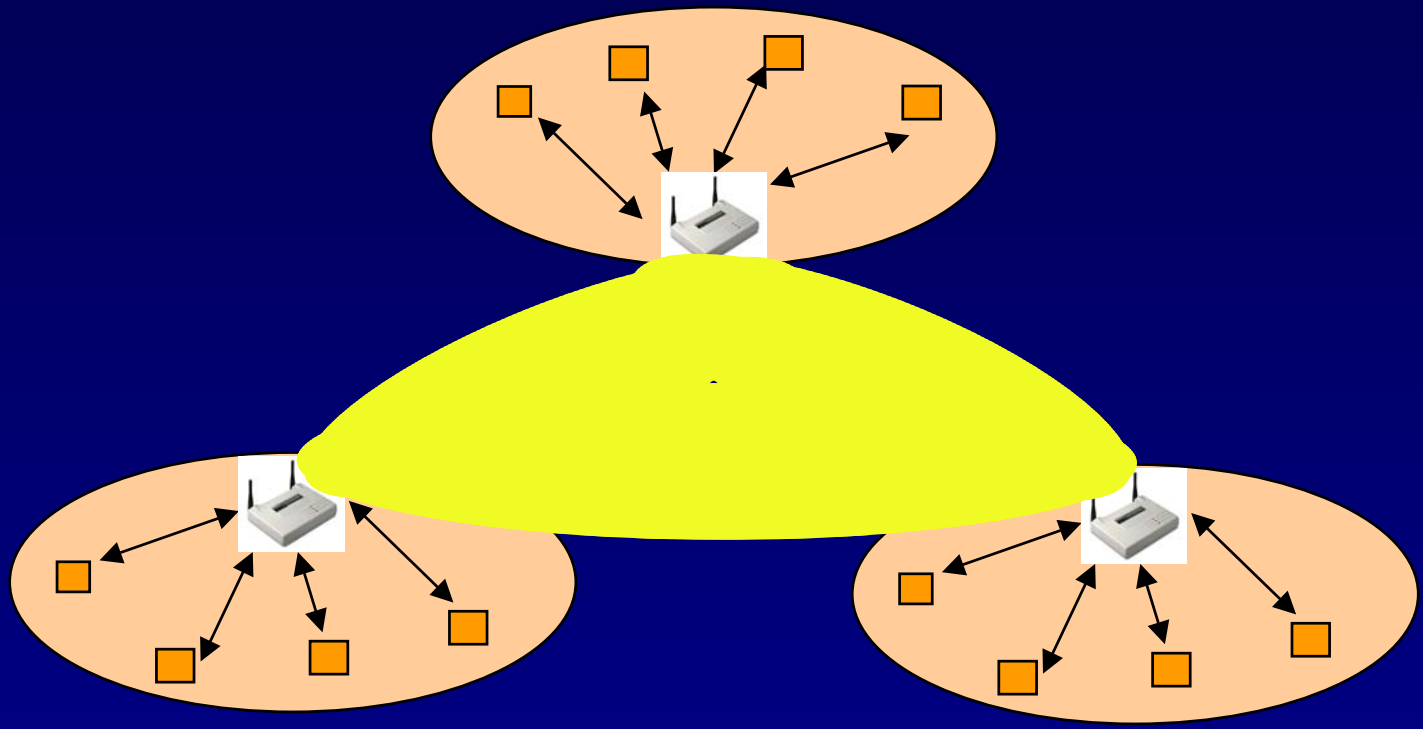
Infrastructure Basic Service Set (BSS)



- AP provides
  - connection to wired network
  - relay function
- stations not allowed to communicate directly

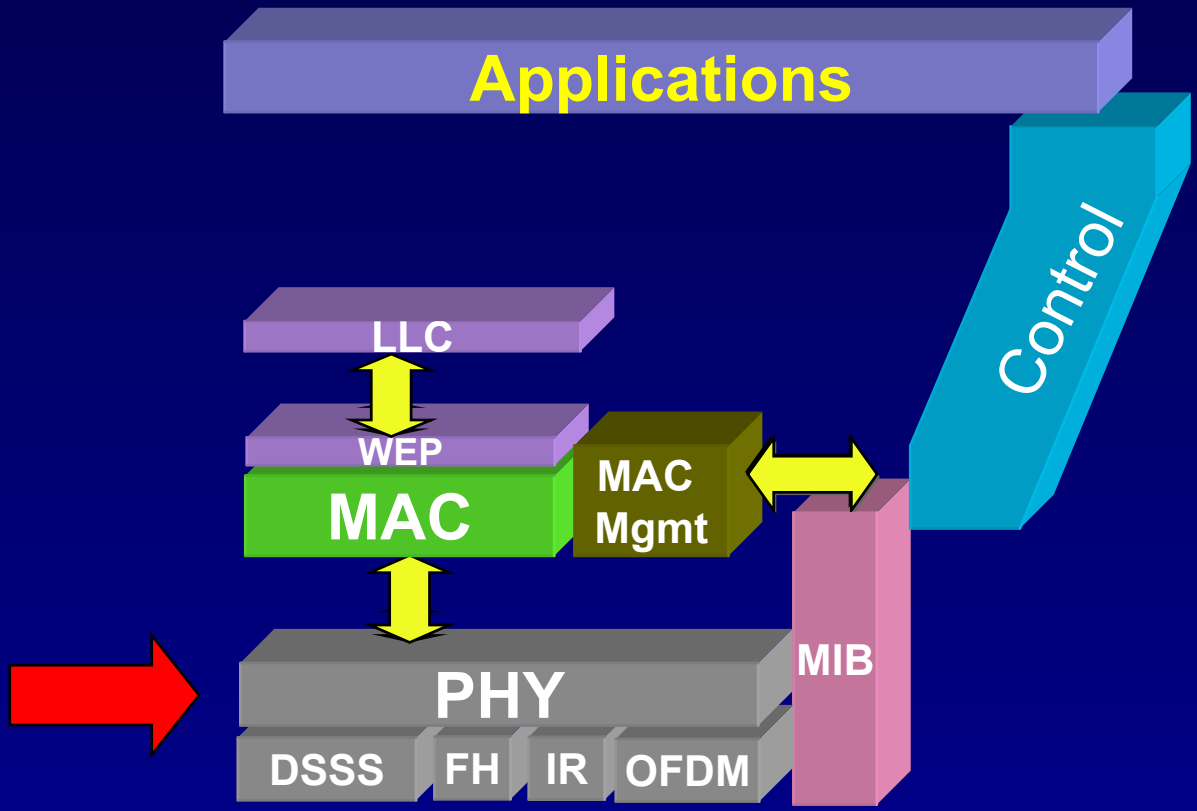
Extended Service Set

ESS: a set of BSSs interconnected by a distribution system (DS)

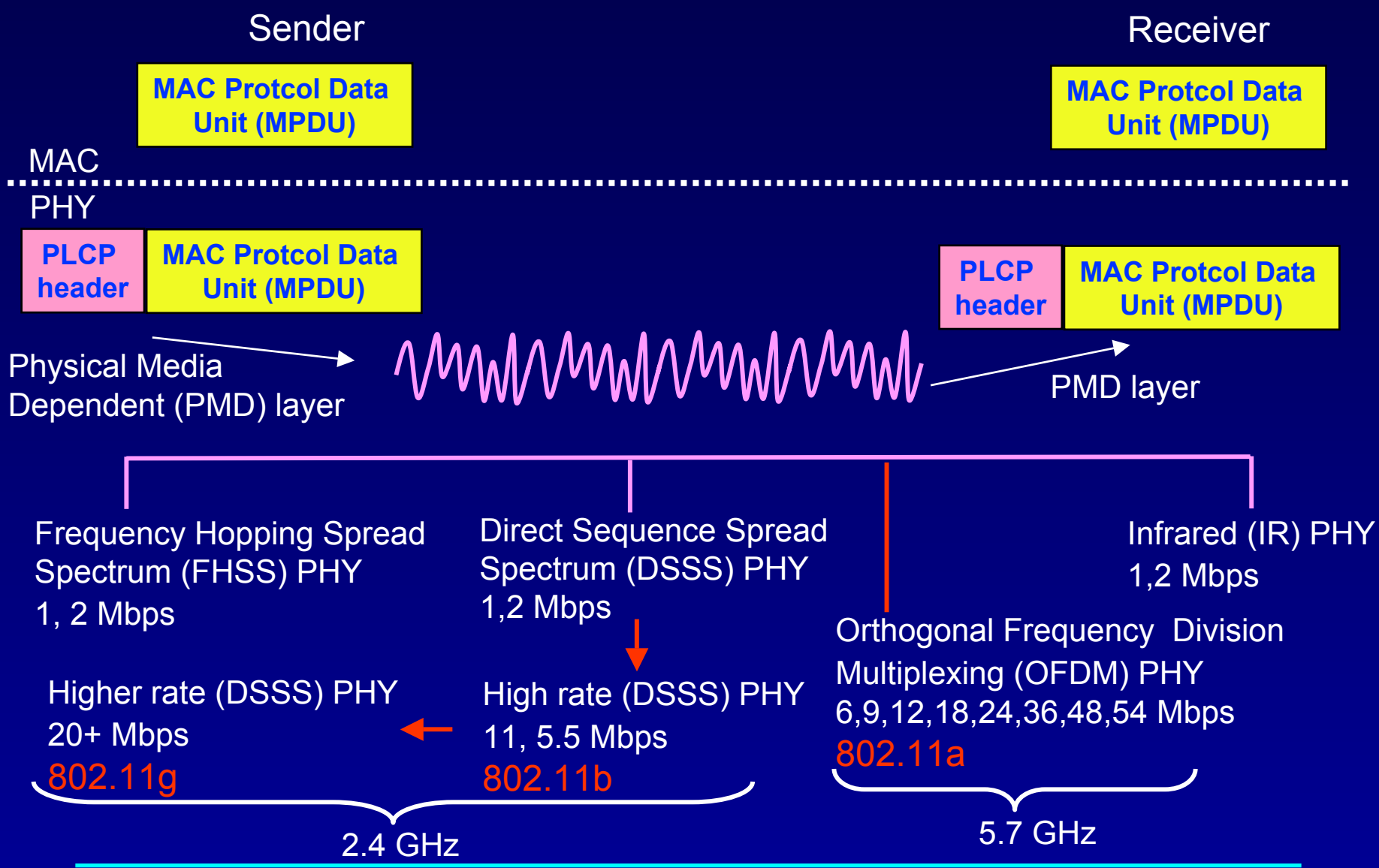


- ESS and all of its stations appear to be a single MAC layer
- AP communicate among themselves to forward traffic
- Station mobility within an ESS is invisible to the higher layers

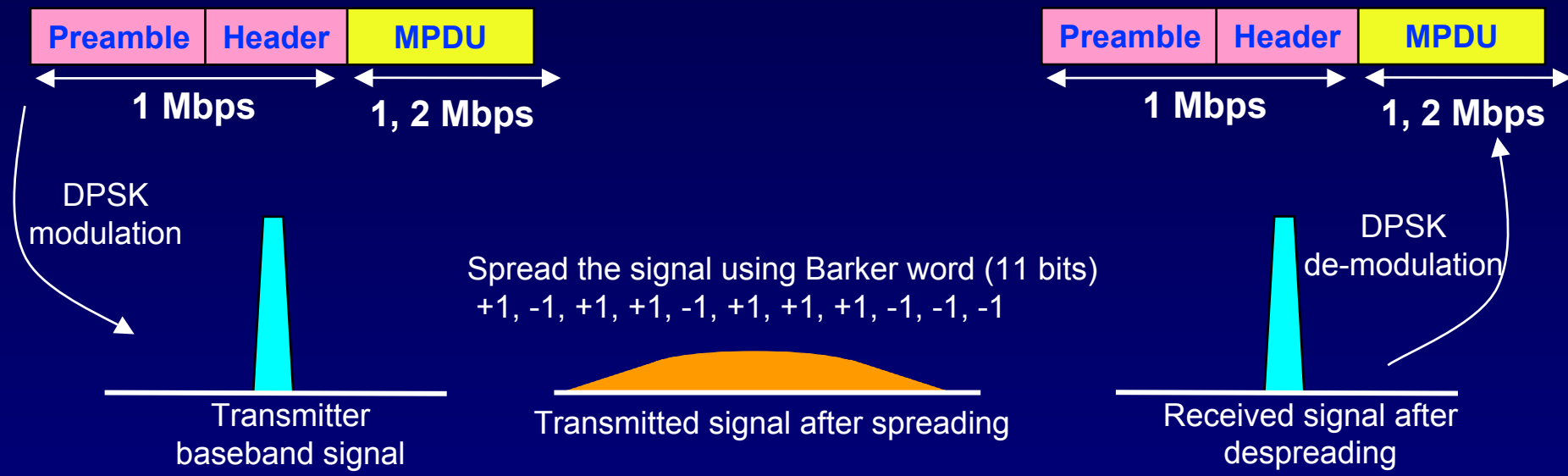
802.11 PHY


Applications
Control
LLC
WEP
MAC
MAC
Mgmt
MIB
PHY
DSSS
FH
IR
OFDM

802.11 PHY

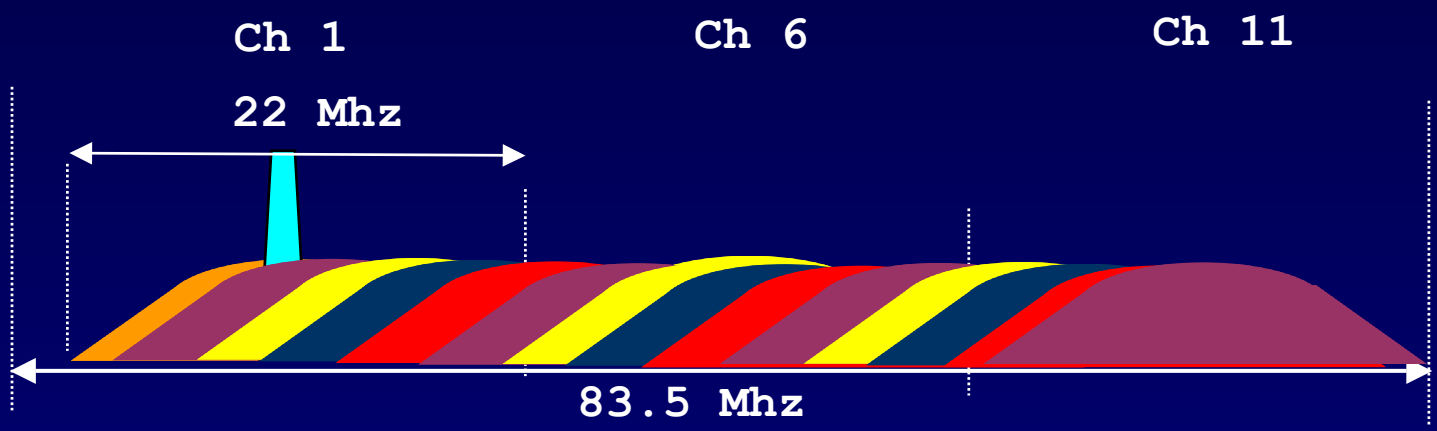

Sender
Receiver
MAC Protcol Data Unit (MPDU)
MAC Protcol Data Unit (MPDU)
MAC
PHY
PLCP header
MAC Protcol Data Unit (MPDU)
PLCP header
MAC Protcol Data Unit (MPDU)
Physical Media Dependent (PMD) layer
PMD layer
Frequency Hopping Spread Spectrum (FHSS) PHY
1, 2 Mbps
Direct Sequence Spread Spectrum (DSSS) PHY
1,2 Mbps
Infrared (IR) PHY
1,2 Mbps
Orthogonal Frequency Division Multiplexing (OFDM) PHY
6,9,12,18,24,36,48,54 Mbps
802.11a
Higher rate (DSSS) PHY
20+ Mbps
802.11g
High rate (DSSS) PHY
11, 5.5 Mbps
802.11b
2.4 GHz
5.7 GHz

DSSS PHY



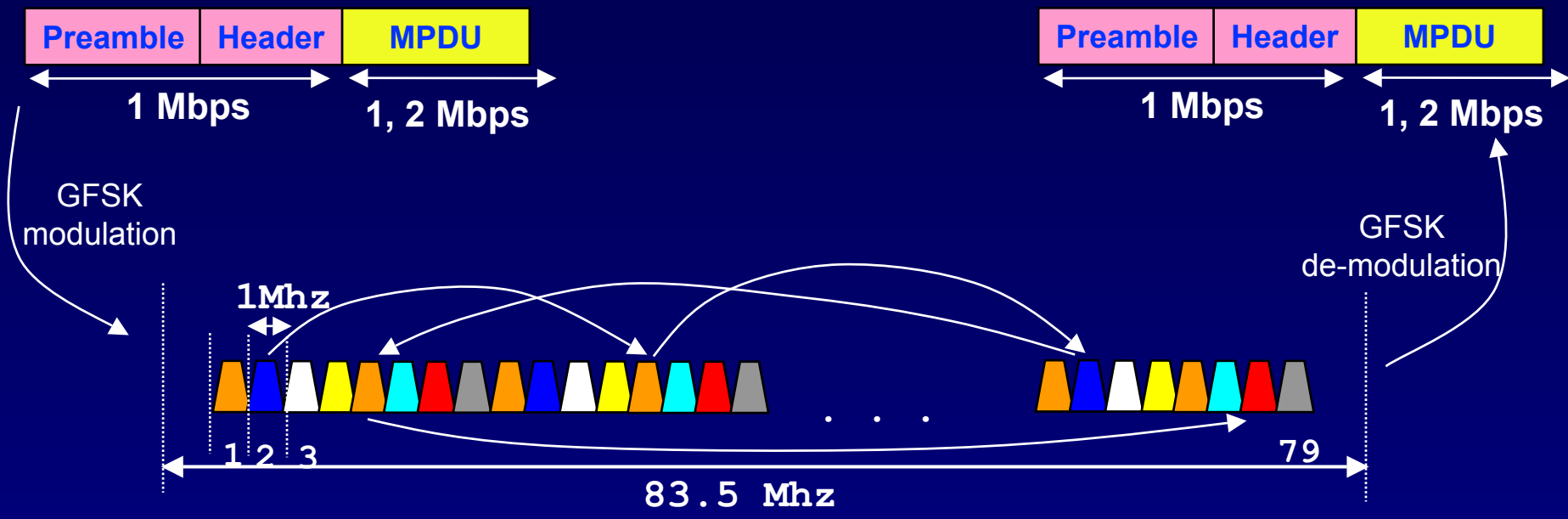
- Baseband signal is spread using Barker word (10 dB processing gain)
- Spread signal occupies approximately 22 Mhz bandwidth
- Receiver recovers the signal by applying the same Barker word
- DSSS provides good immunity against narrowband interferer
- CDMA (multiple access) capability is not possible

DSSS PHY



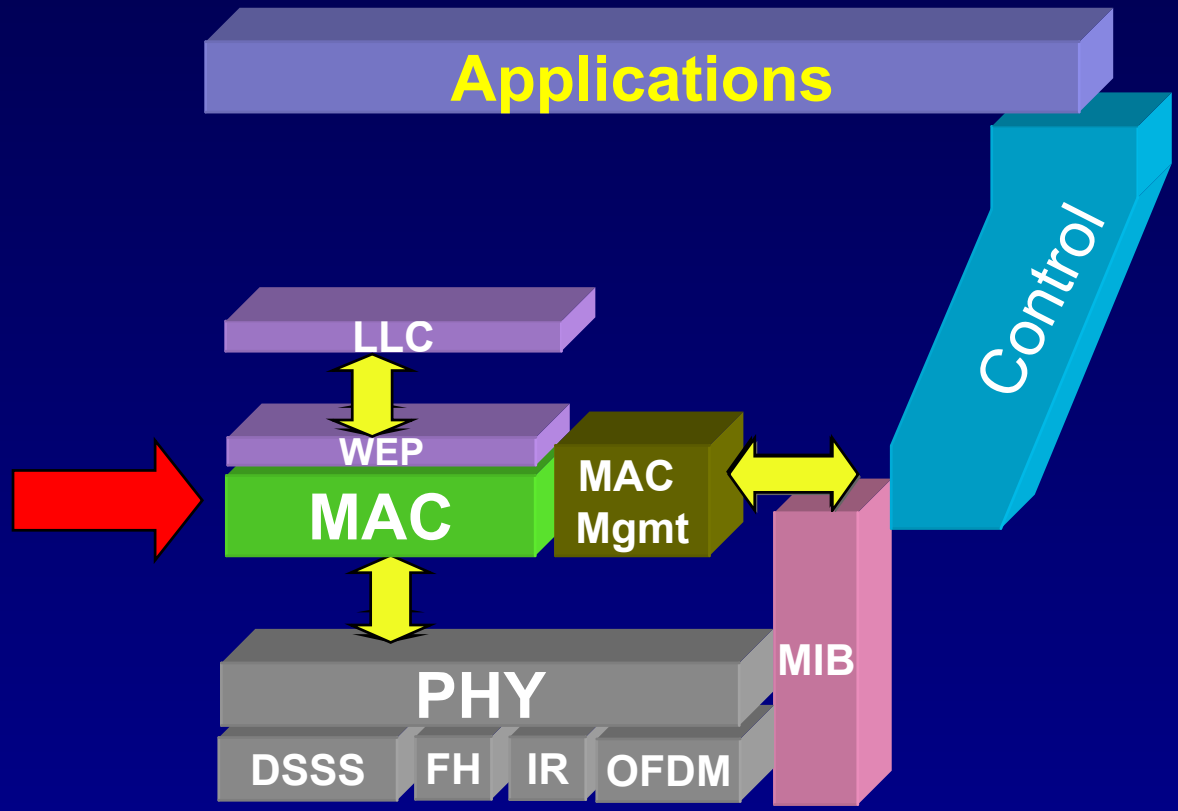
- Direct sequence spread spectrum
  - Each channel is 22 Mhz wide
- Symbol rate
  - 1 Mb/s with DBPSK modulatio
  - 2 Mbps with DQPSK modulation
  - 11, 5.5 Mb/ps with CCK modulation
- Max transmit power
  - 100 Mw

FHSS PHY



- Hopping sequences are grouped into three sets
  - Each set contains 26 hopping sequences (North America)
  - 2.5 hops/sec, minimum hop distance = 6 Mhz
- GFSK modulation
  - 1, 2 Mb/s symbol rate

802.11 MAC


Applications
Control
LLC
WEP
MAC
MAC Mgmt
MIB
PHY
DSSS
FH
IR
OFDM

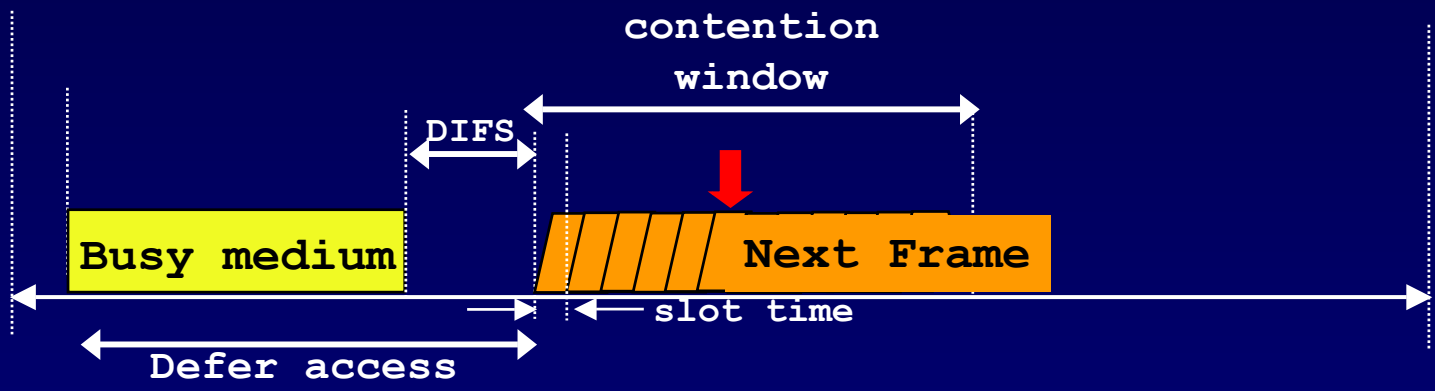
802.11 MAC : Design goals

- Single MAC to support multiple PHYs
  - Support multiple channel PHYs
- Robust against interference
- Cope with hidden nodes
- Support for time bounded service, QoS
- Should be scalable and stable at high loads
- Need provisions for Power Saving Modes
- Need provisions for Privacy and Access Control

802.11 MAC

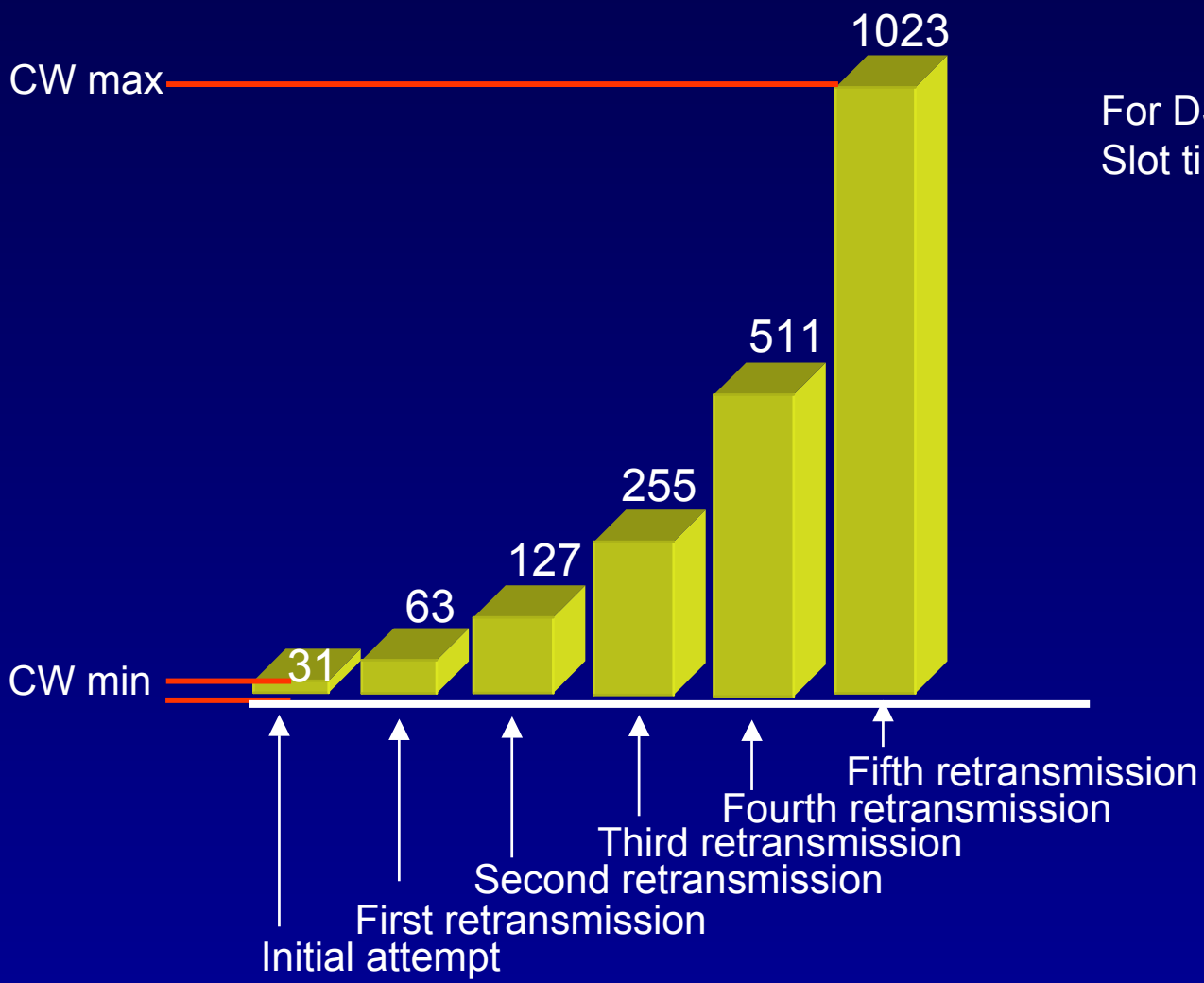
- Carrier sensing (CSMA)
  - Rules:
    - carrier ==> do not transmit
    - no carrier ==> OK to transmit
  - But the above rules do not always apply to wireless.
    - Solution: RTS/CTS
- Collision detection (CD)
  - Does not work over wireless
  - Therefore, use collision avoidance (CA)
    - random backoff
    - priority ack protocol

802.11 MAC protocol: CSMA/CA



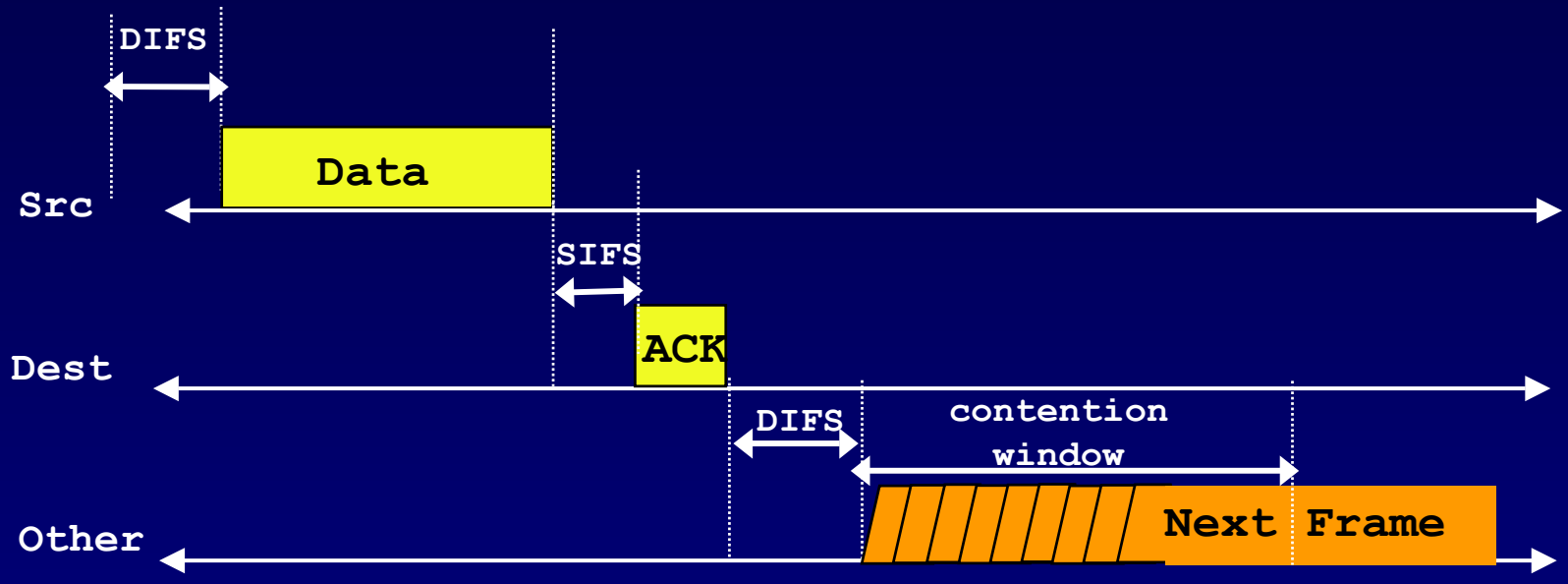
- Use CSMA with collision Avoidance
  - Based on carrier sense function in PHY called Clear Channel Assessment (CCA)
- Reduce collision probability where mostly needed
- Efficient backoff algorithm stable at high loads
- Possible to implement different fixed priority levels

802.11 MAC : Contention window



For DSSS PHY
Slot time = 20 μs

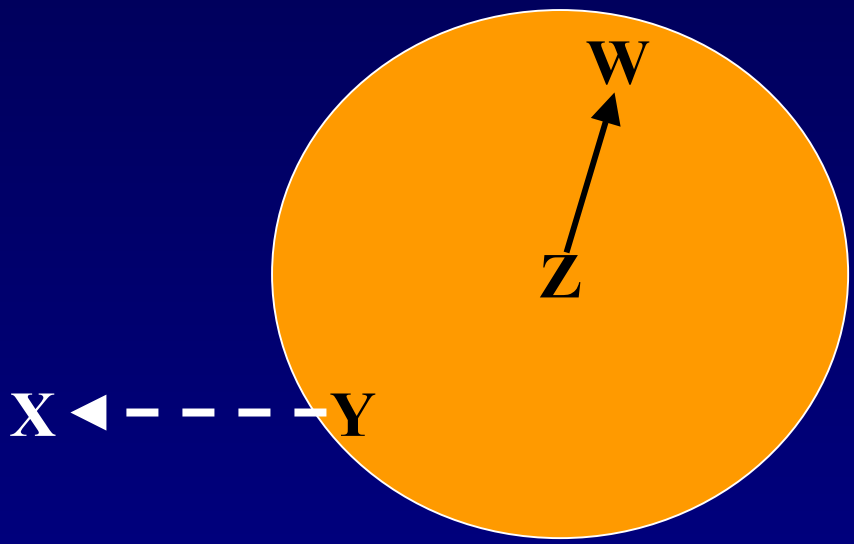
CSMA/CA + ACK protocol



- Defer access based on carrier sense
- Direct access when medium is sensed free longer than DIFS
- Receiver of directed frames to return an ACK immediately when CRC is correct
  - When no ACK received then retransmit frame after a random backoff

Problems with carrier sensing

Exposed terminal problem



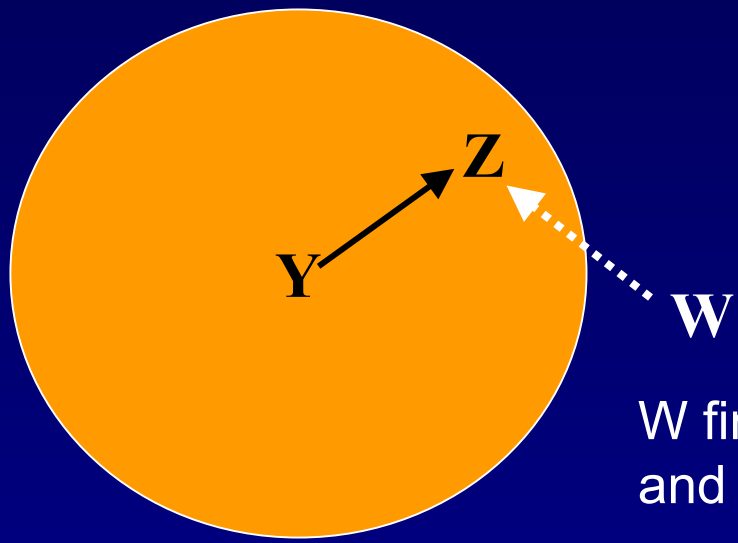
Z is transmitting to W

Y will not transmit to X
even though it cannot interfere

Presence of carrier ==/=> hold off transmission

Problems with carrier sensing

Hidden terminal problem

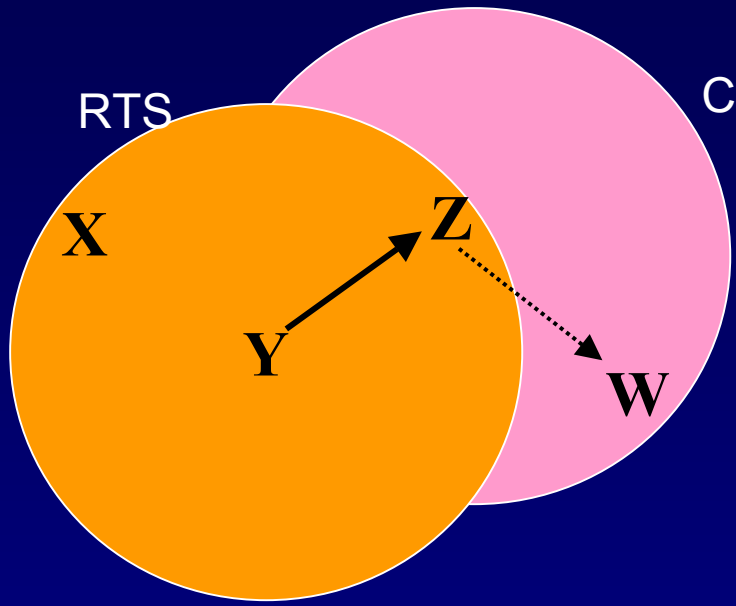


W finds that medium is free and it transmits a packet to Z

no carrier ==/=> OK to transmit

Solving Hidden Node problem with RTS/CTS

- listen RTS
- wait long enough for the requested station to respond with CTS
- if (timeout) then ready to transmit

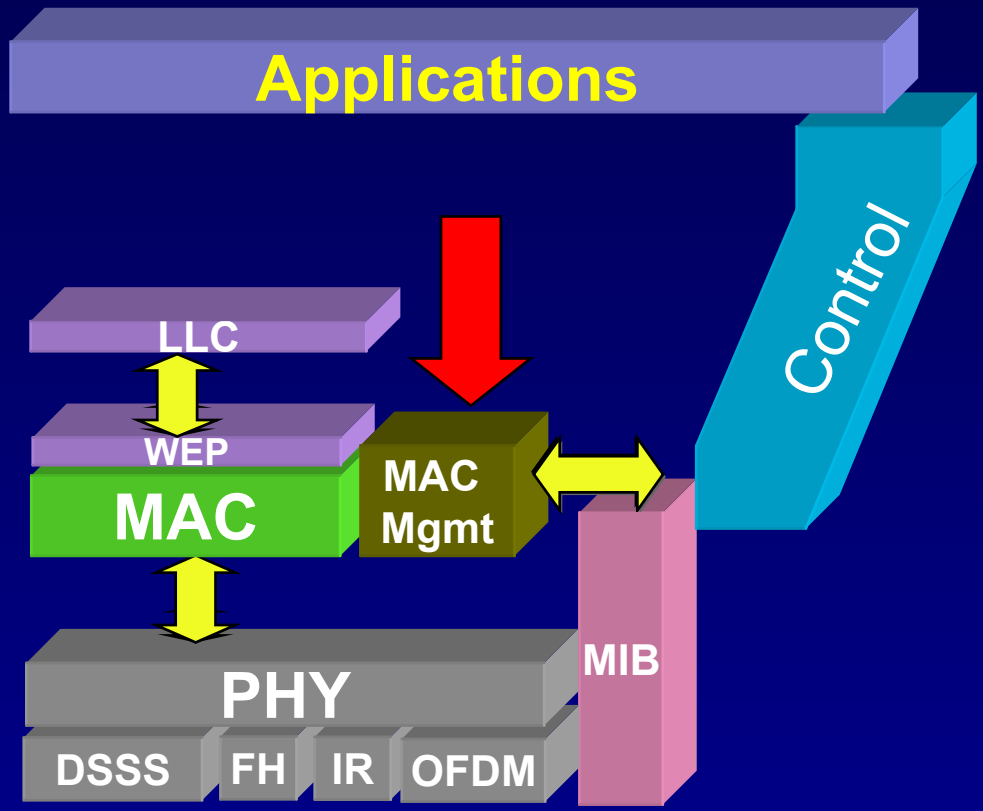


- listen CTS
- wait long enough for the transmitter to send its data

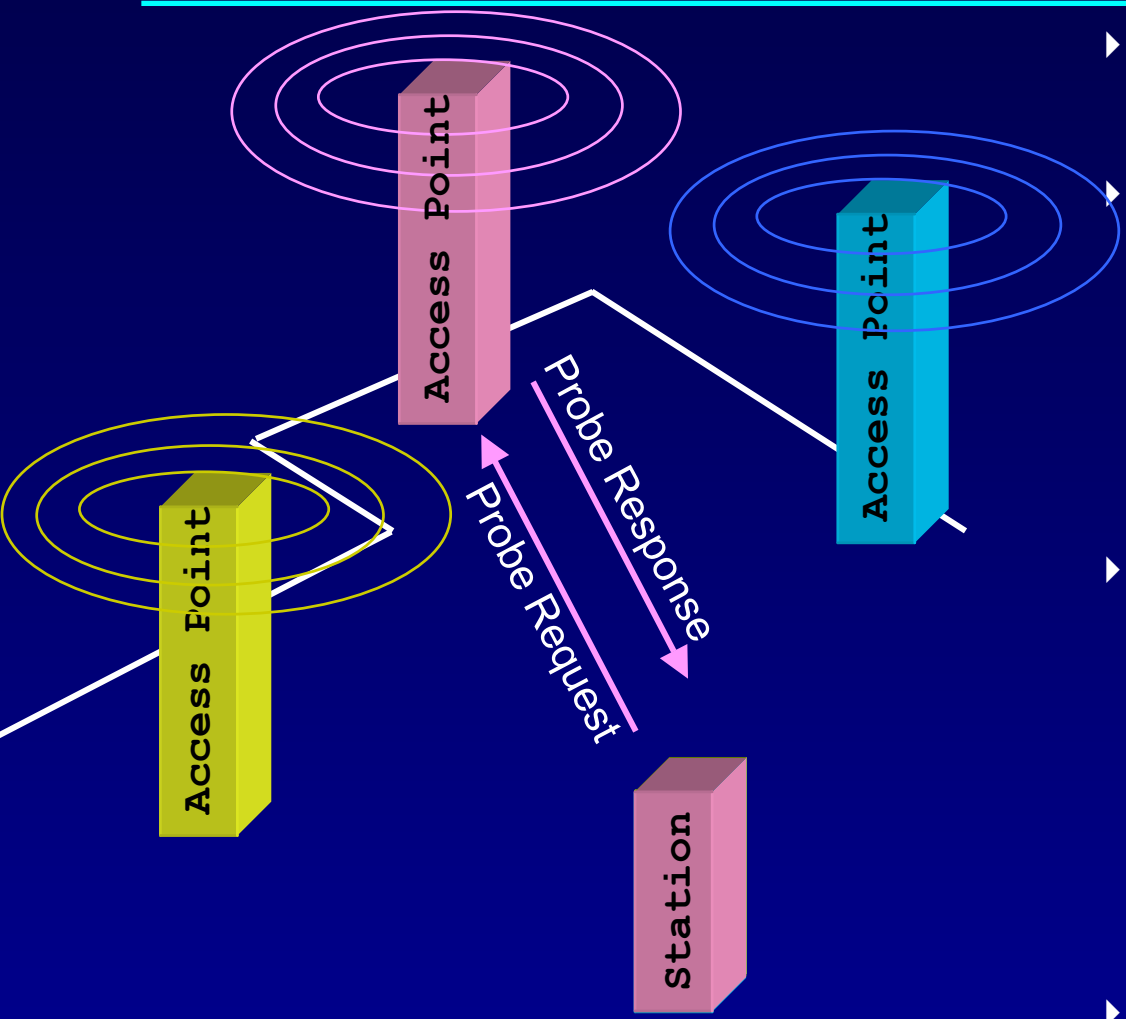
listen RTS ==> transmitter is close to me
listen CTS ==> receiver is close to me

Note: RTS/CTS does not solve exposed terminal problem. In the example above, X can send RTS, but CTS from the responder will collide with Y's data.

802.11 MAC sublayer Management

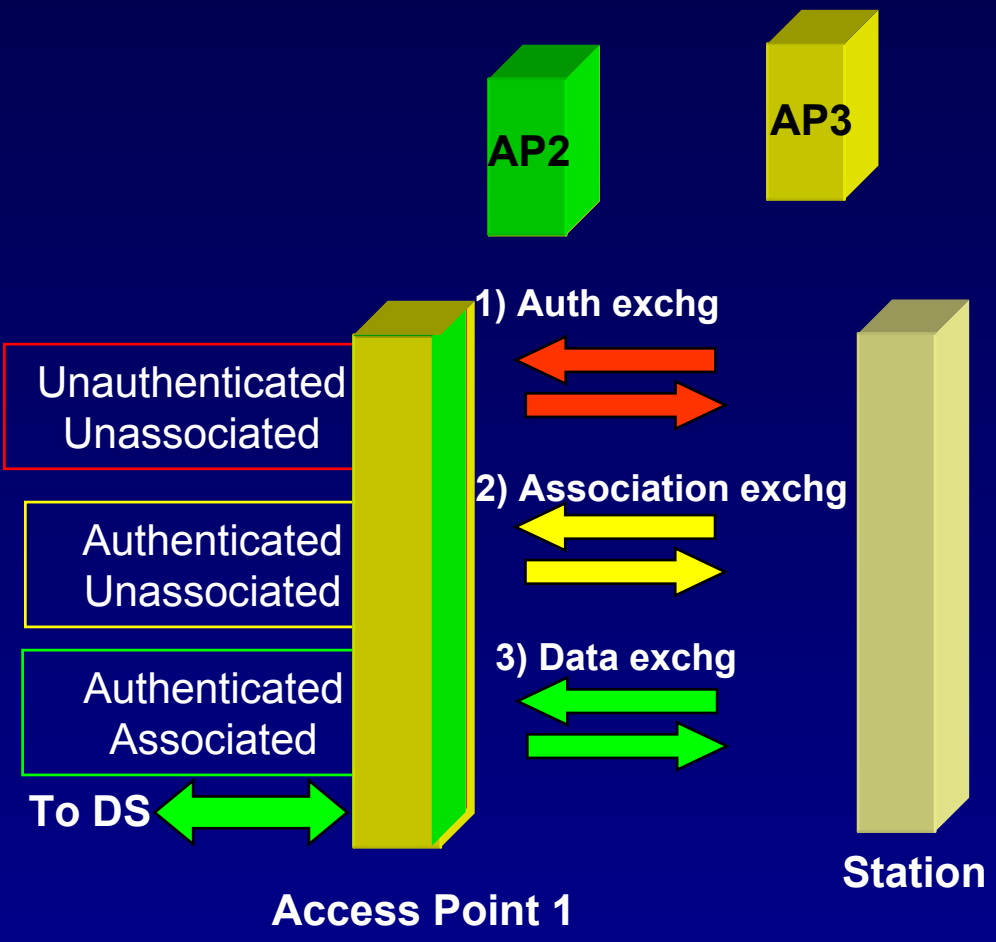


MAC Management: Beacon & Probes



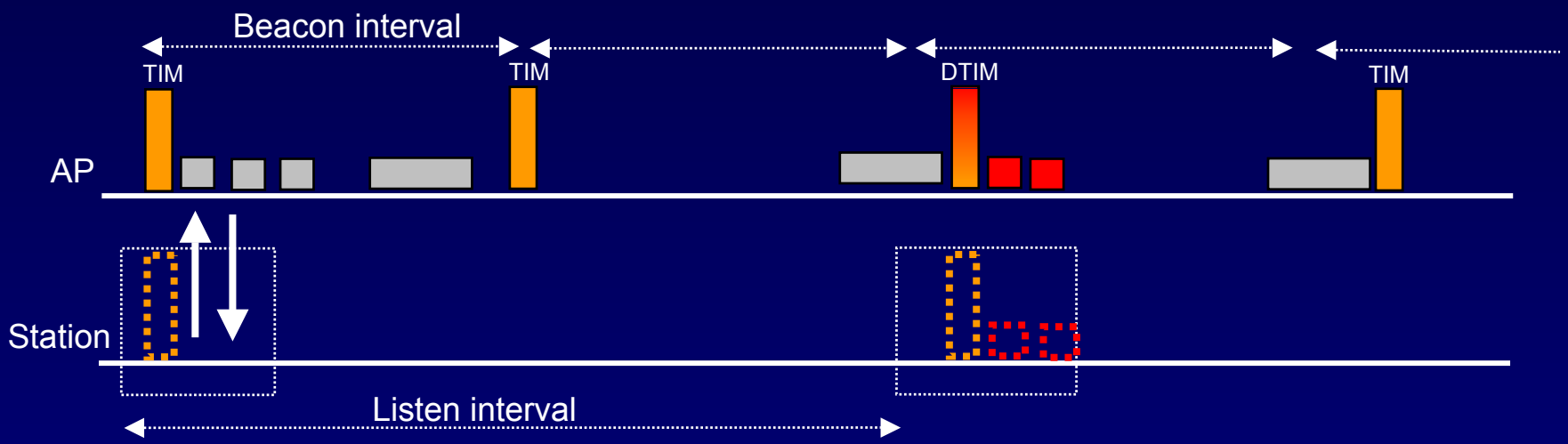
- A station can first scan the network and discover the presence of BSS in a given area
- Scanning
  - Passive
    - listen for beacons on each channel
  - Active
    - send probe and wait for response on each channel
- Beacon and probe response packets contain:
  - AP timing information,
  - Beacon period,
  - AP capability information,
  - SSID,
  - PHY parameter set,
  - Traffic Indication Map (TIM)
- SSID (Service set identifier)
  - identifies an ESS or IBSS

MAC Mgmt : Authentication & Association



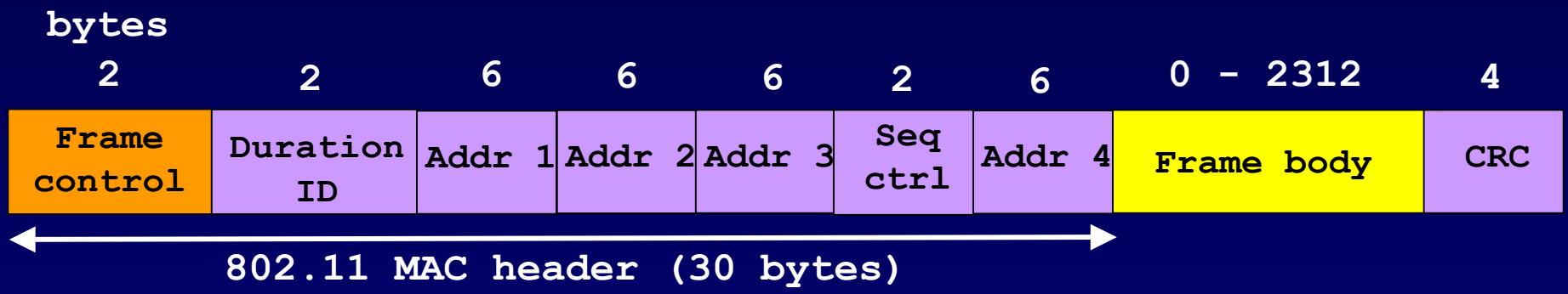
- With respect to an access point, a station can be in one of the following three states
  - Unauthenticated/Unassociated
  - Authenticated/Unassociated
  - Authenticated/Associated
- A station can pre-authenticate with several access points in advance to speedup roaming
- A station can be associated with only one AP at a given time
- Association state is used by the distribution system to figure out the current location of the station within the ESS.

MAC Mgmt : Power Management



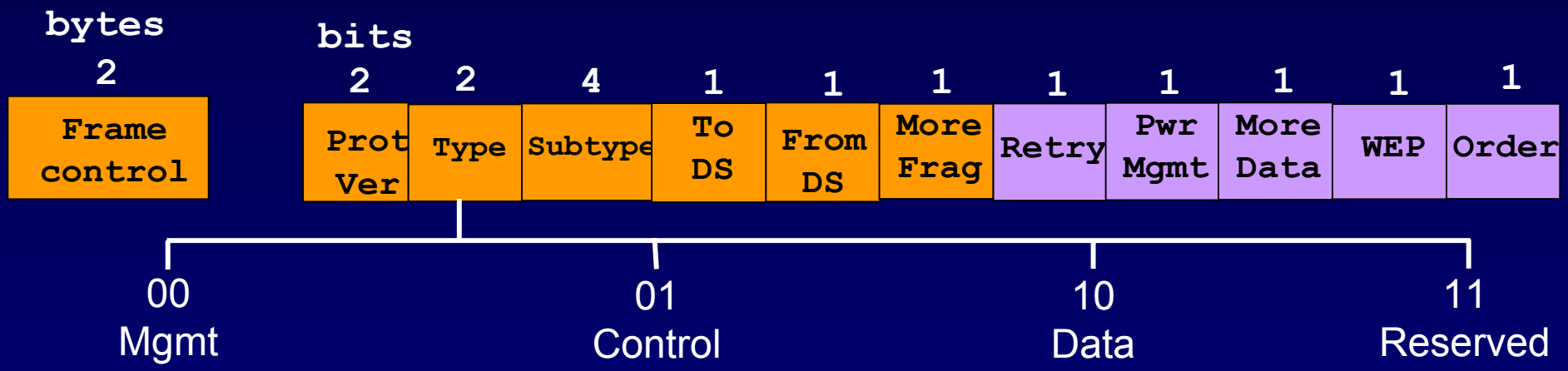
- A station which is synchronized with an AP clock can wake up periodically to listen for beacons
- Beacon packets contain Traffic Indication Map (TIM), a bit vector, which indicates whether a station has a packet buffered at AP
- The station sends a PS-Poll message to the AP asking the AP to release buffered packets for the station
- All broadcast and multicast frames are transmitted following beacons with DTIM flag set

802.11 Frame Format



- 802.11 frame has more fields than other media type frames
- 30 bytes frame header appears too long!
- All fields are not present in all frames

Frame Control Field

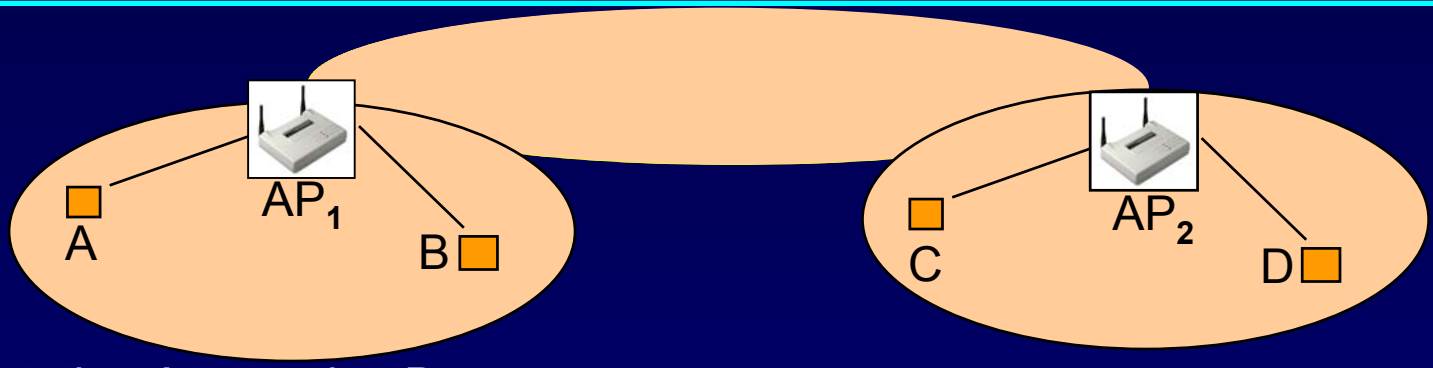


Association req
Association resp
Re-association req
Re-association resp
Probe req
Probe resp
Beacon
Announcement Traffic Indication Request (ATIM)
Disassociation
Authentication
De-authentication

Power save (PS)-poll
Request to Send (RTS)
Clear to send (CTS)
Acknowledgement (ACK)
Contention free (CF)-END
CF-END + CF-ACK

Data
Data + CF+ACK
Data + CF-Poll
Data + CF-ACK + CF-Poll
Null
CF-ACK
CF-Poll
CF-ACK + CF-Poll

Data Forwarding Scenarios



station A to station B

- There is no guarantee that B will be able to hear A's transmission
- A must first send the packet to AP_1
- AP_1 will then forward that packet to B
- Need space for holding three addresses in the packet header

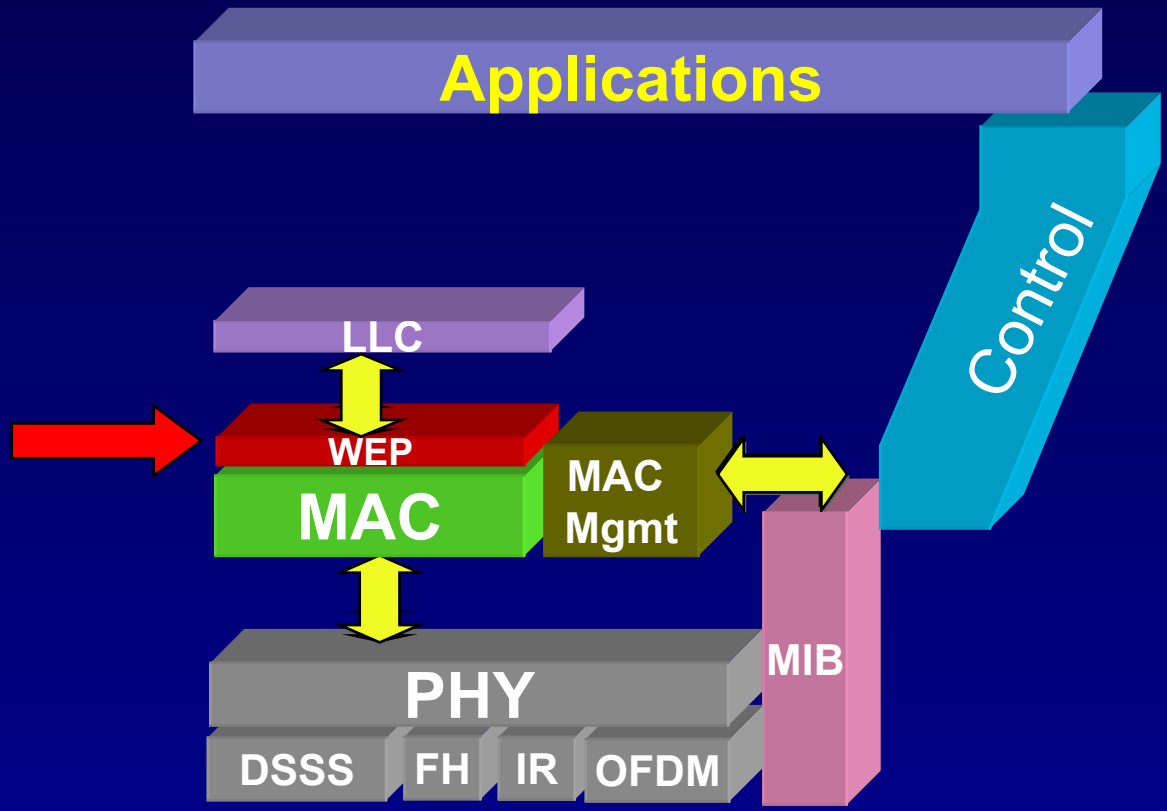
station A to station C

- A does not know whether C is associated with AP_1 or with another AP
- A must first send the packet to AP_1
- AP_1 will use the DS to forward that packet to AP_2

station A to station C via wireless DS

- Same as above except that the transmitted frame from AP_1 to AP_2 will contain four addresses

802.11 Privacy and Authentication

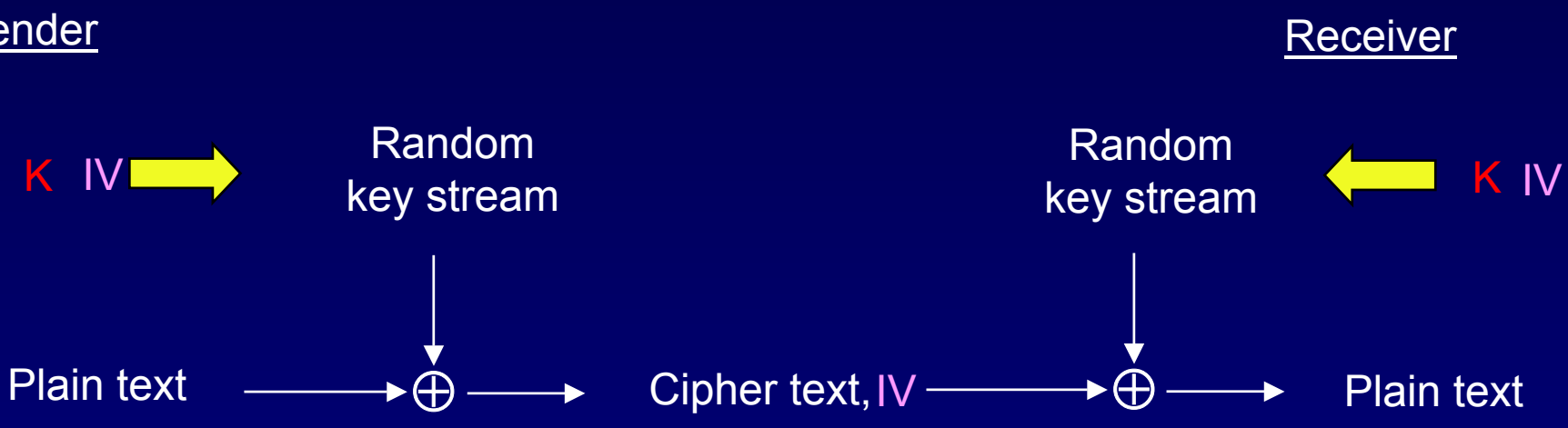


Wired Equivalent Privacy (WEP)

- Design Objectives
  - Confidentiality
    - Prevent others from eavesdropping traffic
  - Data Integrity
    - Prevent others from modifying traffic
  - Access Control
    - Prevent unauthorized network access

Provide same level of security as a physical wire

WEP design: adding privacy

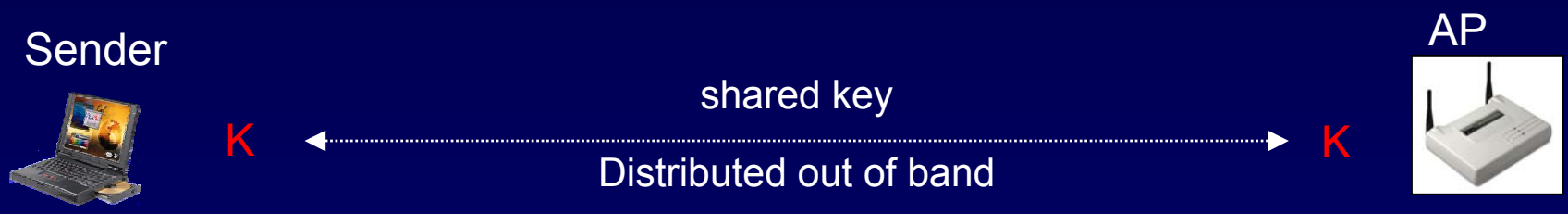


- A secret key is shared between a sender and a receiver
- Using the secret key the sender generates a random key stream
- XOR plain text with the random key stream
- XOR the cipher text with the same random key stream to recovers the plain text
- An eavesdropper cannot compute the plain text by inspecting the cipher text
- New key streams are refreshed periodically
  - Use initialization vector (IV) in conjunction with shared key
  - transmit IV in clear text along with the cipher text

WEP design: adding data integrity

- The problem is that cipher text can be modified without any knowledge of the key
  - Just flip some bits in the cipher text
  - After decrypting the cipher text, receiver will not know that the plain text has been corrupted
- Solution:
  - Computer 32 bit CRC of plain text and append it with plain text before generating the cipher text
  - If cipher text is modified, CRC check will fail and the frame will be discarded

WEP design: adding Authentication

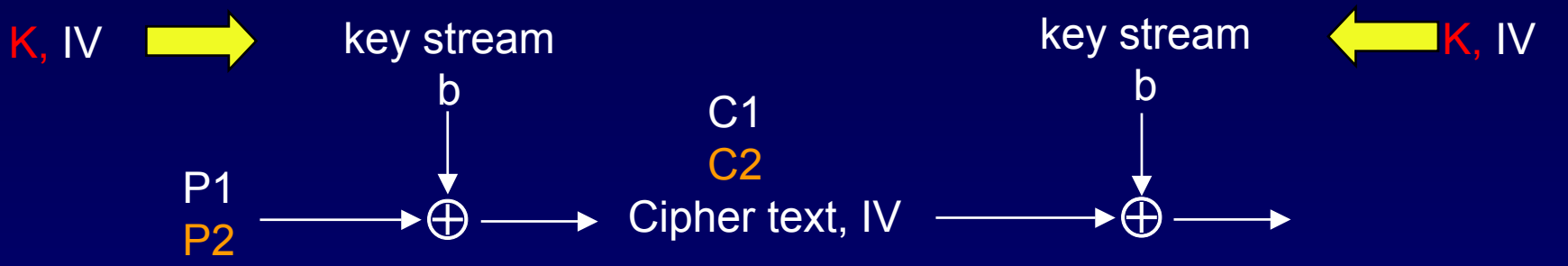


Summary

- Shared secret keys are distributed out of band
- AP sends a challenge to the station
- Station responds with a WEP encrypted packet
- AP verifies station's response

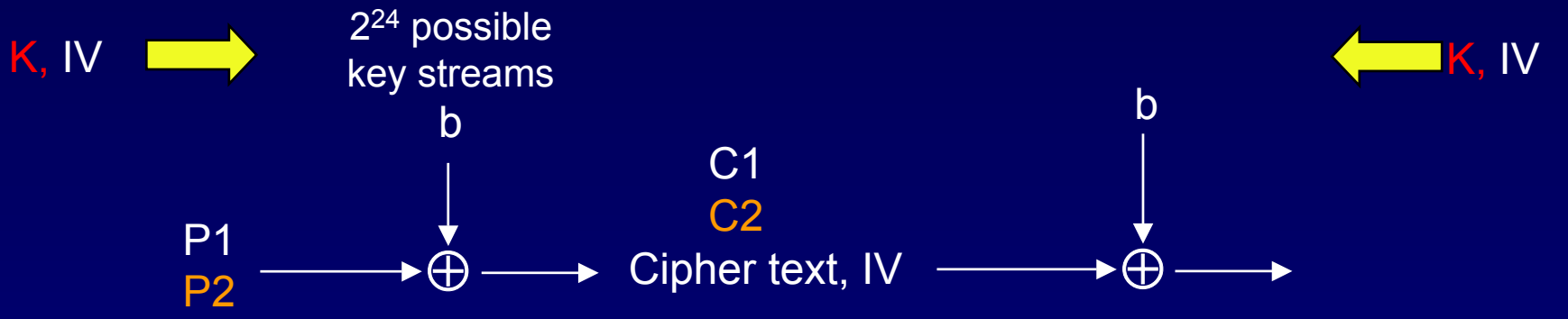
Where is the problem ?

Problem #1: improper use of stream ciphers



- Two messages should never be encrypted using the same key streams
- Suppose P1 and P2 are encrypted using the same key stream
  - C1 = P1 XOR b
  - C2 = P2 XOR b
- Adversary can compute C1 + C2 = P1 + b + P2 + b
  = P1 + P2
- Usually XOR of two plain texts is enough to recover both plain texts
- Moreover, if one plain text is known other can be computed trivially

Key stream reuse in WEP

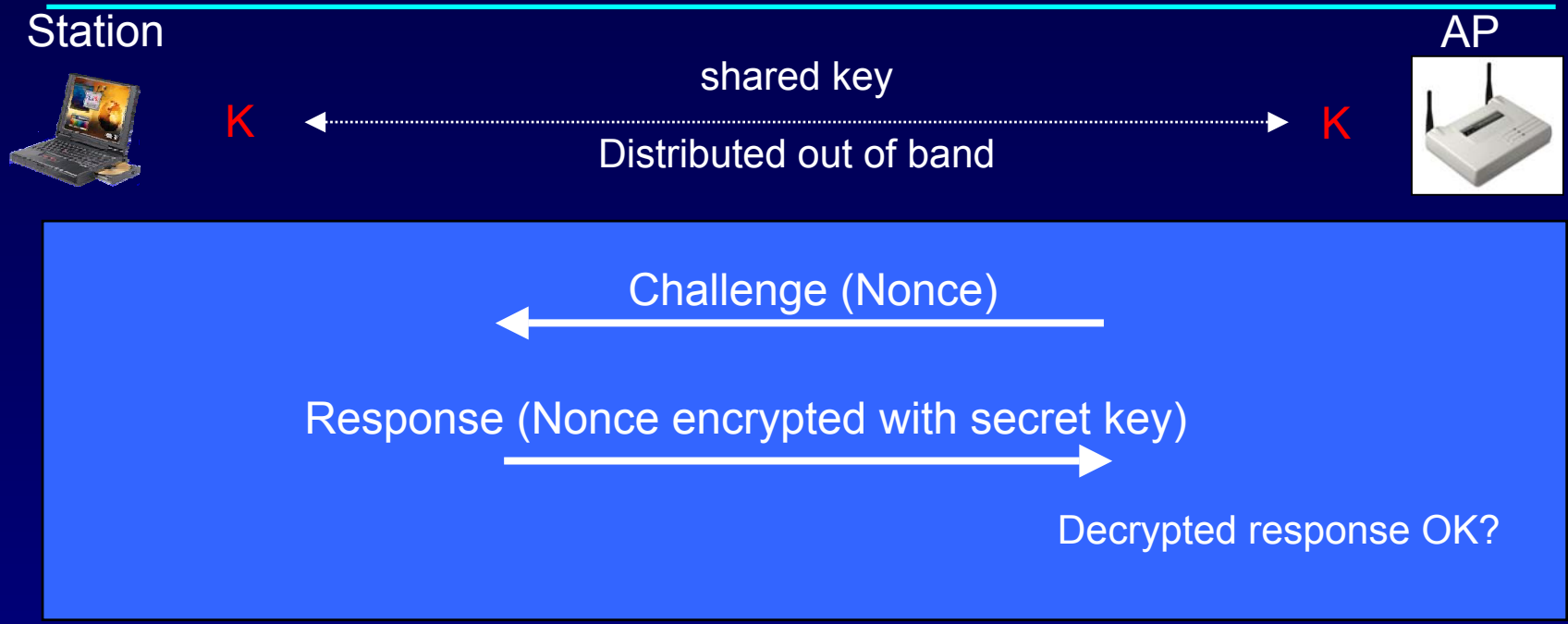


- Key stream is a function of secret key and initialization vector
- IV vector is only 24 bits long; since there are only 16 million combinations, eventually key streams will be recycled
- Since IV vector is transmitted in clear text, Key stream reuse is easy detect by passive eavesdropping
- An eavesdropper can record all instances of key stream reuse
  - Require 1K * 16 million = 16 GB space
- Worse yet, most 802.11 cards when reset start counting IV from 0
  - so, key streams are recycled more frequently

Possible attack: Message decryption

- Inject known plain text in the network by e-mail spamming, or ping
- Passively record encrypted packets
- By computing XOR of known plain text with encrypted packet, it is possible to compute the RC4 key stream that was used to encrypt the known plain text
- Build a dictionary of key streams
  - Map each value to IV to its associated key stream
- Once this dictionary is built, any packet can be decrypted
  - Record the packet
  - Inspect the IV
  - Pull out the key stream associated with the observed IV from the dictionary
  - XOR the key stream with the encrypted packet and obtain the plain text
- The same dictionary can also be used to inject any message in the network

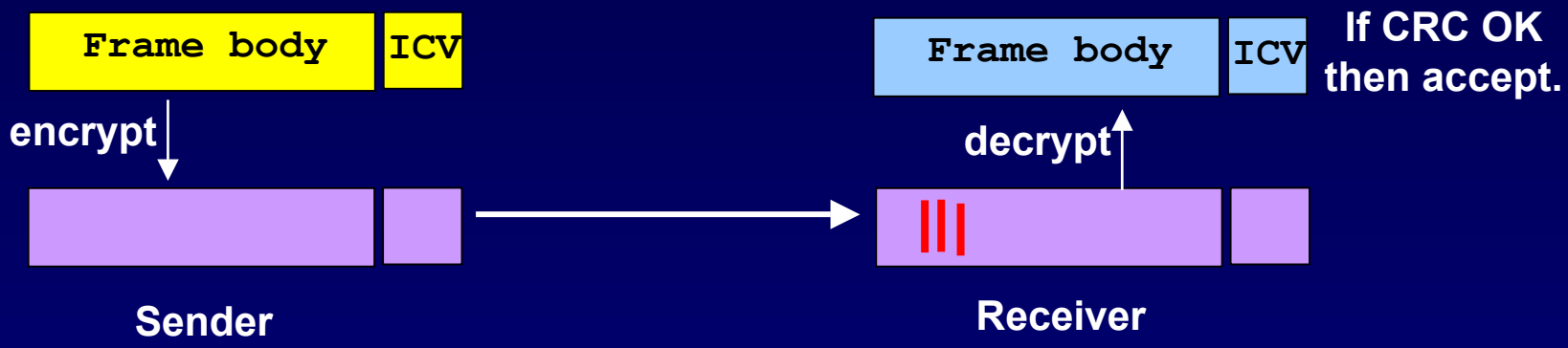
Possible attack: Breaking Authentication



- The previous attack relies on finding a known plain text and its encrypted version to compute the key stream
- By snooping 802.11 Authentication protocol, this pair can be collected for free
- Using this key stream, an adversary station can respond to any new challenge from the AP !

More problems

Problem #2: improper use of CRC

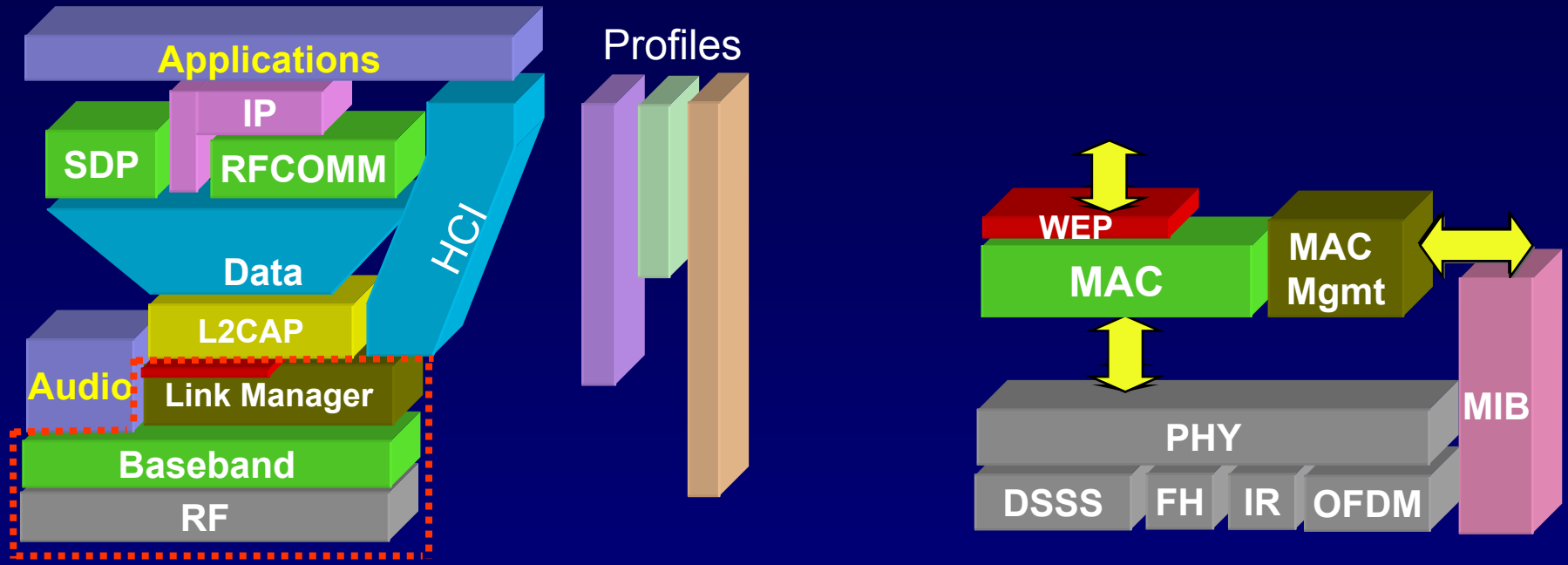


- Integrity check value (ICV) is good at detecting random bit errors, not intentional modifications to the packet
- An adversary can modify an encrypted packet such that those changes cannot be detected by CRC test at the receiver
- This is possible because encryption function (XOR) as well as CRC are both linear operations
  - (M, c(M)) XOR (R, c(R)) = (M XOR R, c(M XOR R))
- The modified message after decryption will pass the CRC test !

WEP current status

- Note that attacks don't try to deduce the key. Knowledge of key stream is enough to launch all sorts of attacks
- Possible Solutions
  - Long IV's which never repeat for the lifetime of the shared secret
  - Replace CRC by a strong message authentication code which depends on the key and IV
- WEP2 addresses the first problem, but not the other
- A recent paper by Fluhrer, Mantin, and Shamir has discovered many inherent weaknesses in RC4 stream cipher. They have shown that RC4 is completely insecure when used used in a way prescribed by WEP, in which a fixed secret key is concatenated with known IV modifiers.
- 802.11i working group is now looking into using AES instead of WEP. AES will fix both problems of WEP
  - AES is a block cipher
  - AES includes a strong keyed message authentication code
- Bill Arbaugh's web-page (http://www.cs.umd.edu/~waa/wireless.html) is good source of info on this topic.

Bluetooth Vs. 802.11



- Bluetooth is a (top down) market driven consortium
  - Business interests take precedence over technical considerations
  - Designed primarily for voice; data an afterthought
- 802.11 is a (bottom up) open standard effort
  - Good piece of engineering except for WEP
  - Designed primarily for data; voice an afterthought

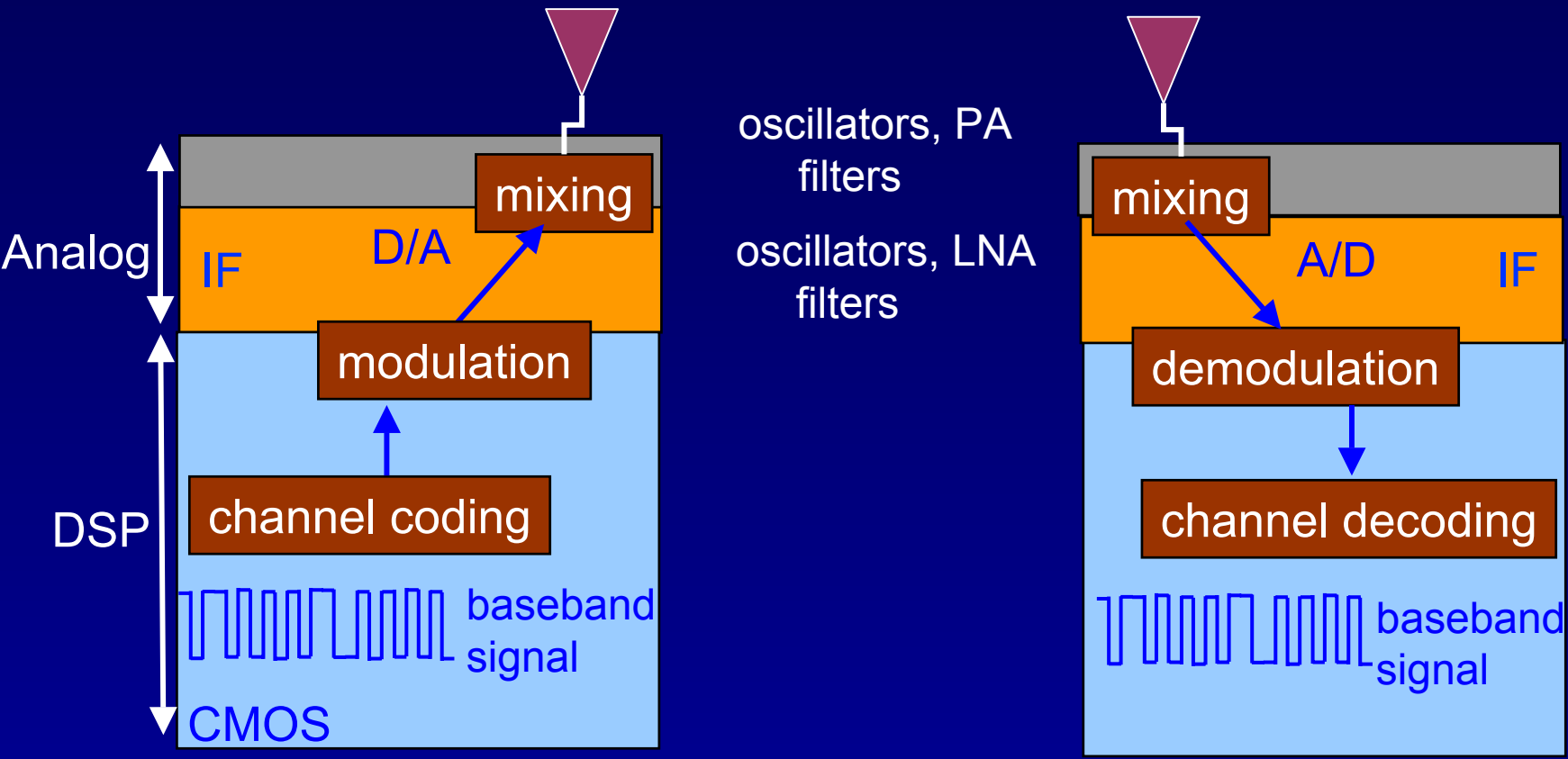
Bluetooth Vs. 802.11: Radio issues

Radio is typically the most costly component in a wireless network interface

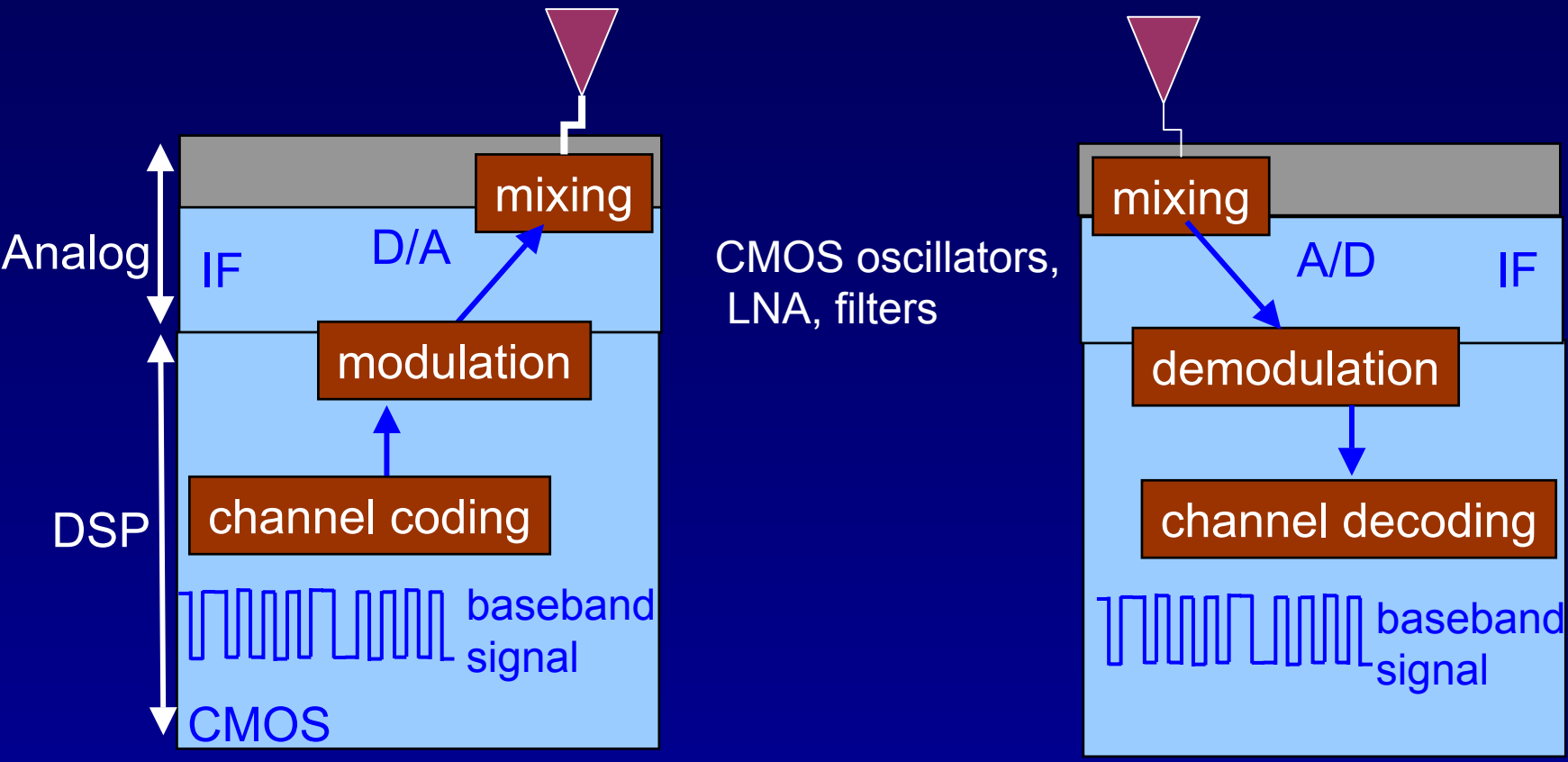
- Bluetooth radio is (will be) inexpensive because
  - It is a frequency hopper (which is relatively easy to build)
  - Its sensitivity is poor
  - It uses very simple modulation technique (GFSK) (requires less silicon)
  - It is possible to package both baseband and radio in a single chip
  - Potentially market for Bluetooth radios is (will be?) large if every mobile phone vendors decide to embed Bluetooth in their products
- 802.11 DSSS radios are costly today, but
  - if market for 802.11 continues to grow, their price may become competitive to Bluetooth
  - DSSS radios are superior to Bluetooth in terms of range, speed, BER performance
  - Due to better range, it may be cheaper to cover an area with 802.11
  - 802.11 can be operated at 0 dBm to reduce power consumption

Radio architecture: 802.11 DSSS (typical)

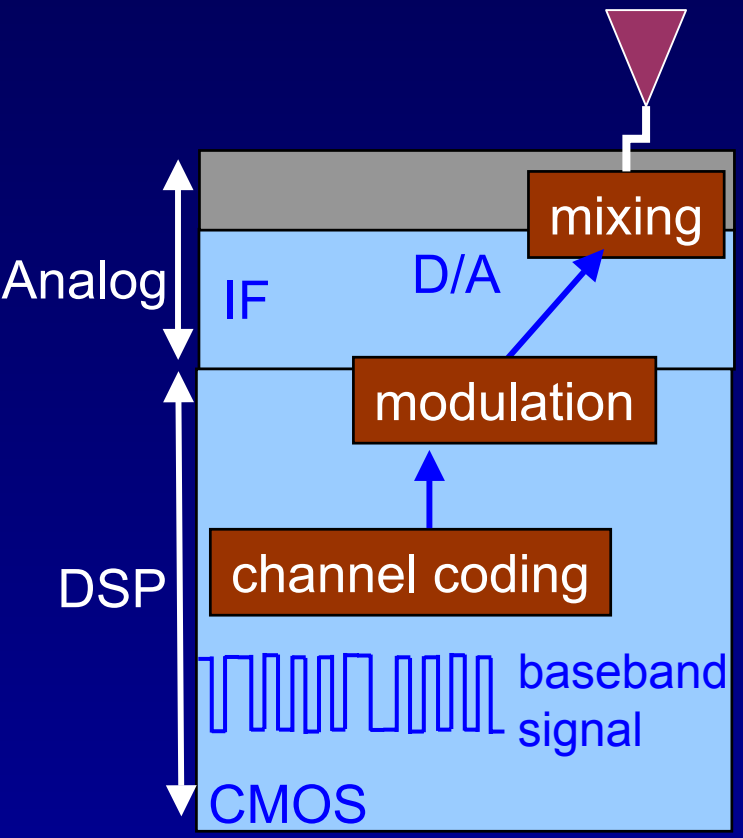
Why is 802.11 radio supposed to be expensive and Bluetooth radio supposed to be cheap?



Radio architecture: Bluetooth



Single chip radio: challenges



- Integrating a low-noise on chip synthesizer
- Handling the wide dynamic range of input interference signals
- Low power draw
- Cross talk between analog/analog and analog/digital circuits
- Achieving good linearity in an integrated filter
- Dealing with very low-level input signals (10μv) in the presence of IC substrate noise
- Dealing with high-level (-5dBm) input signals while keeping a low voltage power supply
- Achieving desired design performance in the presence of 15-20% component variations for R & C

Bluetooth Vs. 802.11: MAC issues

	Bluetooth	802.11
Access Method	TDD Good for voice, but difficult for data	CSMA Good for data, but difficult for voice
Robustness to interference	ARQ	ARQ
Hidden nodes	Not an issue	RTS/CTS
Power Management	Yes	Yes
Power Control	Possible	Not possible
Paging	Possible	Not possible
Scalability	Limited	Stable at high loads
Future safe?	Not sure	Yes

Bluetooth Vs. 802.11: Market issues

	Bluetooth	802.11
Cost	Potential for low cost implementation exists but the market size will eventually determine the price point	Technology advances and market growth can reduce cost, even if tight single integration is not achieved in the near term
Market size	Potentially huge if every consumer electronic device is Bluetooth enabled	It is unlikely that 802.11 will penetrate the cosumer electronic device market in the near future
Form factor	Smaller due to single chip integration	Multi chip solution
Power consumption	Lower due to low power transmitter and tight integration	Will reduce in the future
Interoperability	The biggest problem of Bluetooth at present	802.11 is a more mature technology
Applications	Still looking for a killer app.	TCP/IP

Concluding remarks

- Will Bluetooth survive?
  - Bluetooth is ideal for cable replacement
  - Initial applications of Bluetooth will exploit its point-to-point or point-to-multipoint connectivity feature
  - Attempts to turn it into a LAN technology will face tough competition from 802.11b and 802.11a
  - Multi-hop over Bluetooth is still a technically challenging problem
  - Higher chances of success in Europe and Asia
- 802.11
  - Will continue to grow in
    - Public spaces, home, industry vertical, and enterprise market
  - 802.11 will provide a viable alternative to 3G in public places