Bluetooth

Renato Lo Cigno
www.dit.unitn.it/locigno/teaching

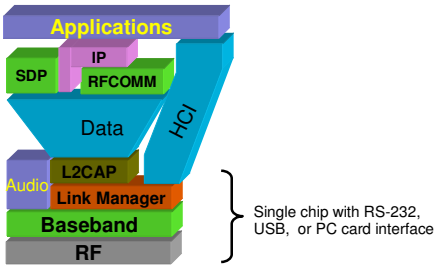
...Copyright

- Thanks: Prof. Mario Gerla, UCLA, for providing most of the material

Technologies

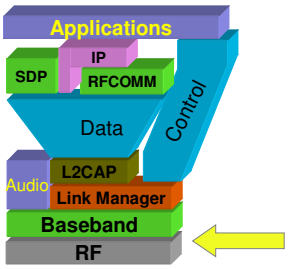
- 802.11
  - Do you know it ☺
- Bluetooth (802.15.1)
  - Master/Slave architecture
  - Optimized for low bandwidth, real time communications
- ZigBee (802.15.4)
  - Meshed architecture
  - Low power consumption
- **All use the same ISM bands**

Bluetooth Specifications

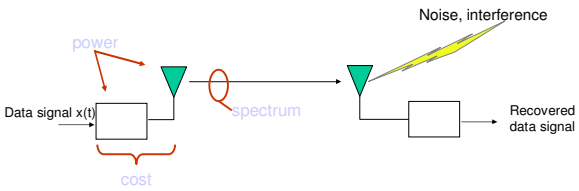


- A hardware/software/protocol description
- An application framework

Bluetooth Radio Specification



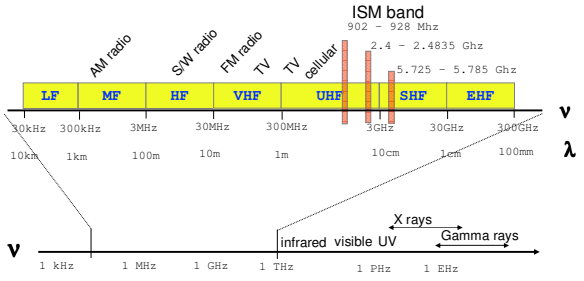
Design considerations



Goal

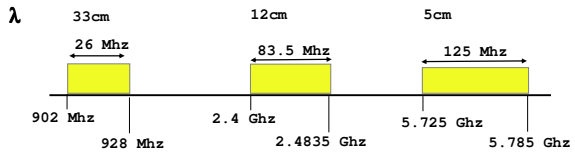
- high bandwidth
- conserve battery power
- cost < $10

EM Spectrum



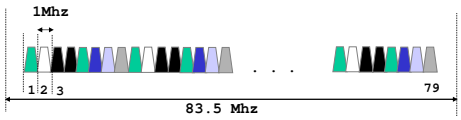
Propagation characteristics are different in each frequency band

Unlicensed Radio Spectrum



cordless phones	802.11	802.11a
baby monitors	Bluetooth	HyperLan
Wireless LANs	Microwave oven	

Bluetooth radio link

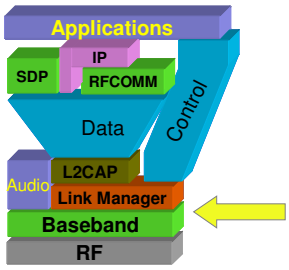


- frequency hopping spread spectrum
  - 2.402 GHz + k MHz, k=0, …, 78
  - 1,600 hops per second
  - Starting BT1.2 (802.15.1-2005) Advanced FH enables interference-avoidance, suppressing the use of interfered channels
- GFSK modulation
  - 1 Mb/s symbol rate
- transmit power
  - 0 dBm (1mW – 1m)
  - 4 dBm (2.5mw – 10m)
  - 20 dBm (100 mW – 100m) with power control

Bluetooth AFH Operation

- AFH only applied when devices are connected
  - Paging and Inquiry modes use all channels, but are only present when devices are searching for others
- Master Bluetooth device using an adapted channel hopping sequence initiates connections using all 79 channels
  - then updates the channel hopping sequence using the AFH channel map
- The AFH channel map is determined by master measurements and responses from slave devices
- The adapted channel hopping sequence consists of the initial 79 channel hop sequence reduced by the master's AFH channel map
- AFH channel map indicated which RF channels shall be used and which shall be unused
- Number of channels used must be > 20

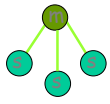
Baseband



Bluetooth Physical link

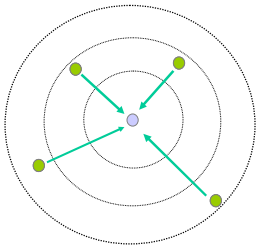
- Point to point link
  - master - slave relationship
  - radios can function as masters or slaves

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

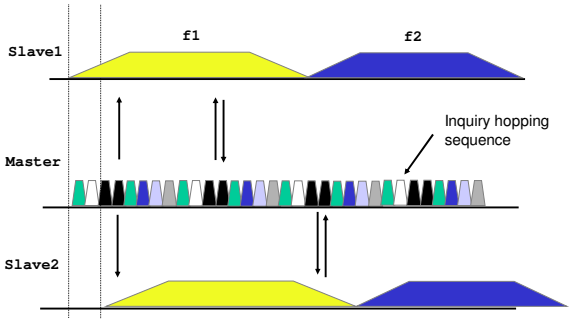


Connection Setup

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

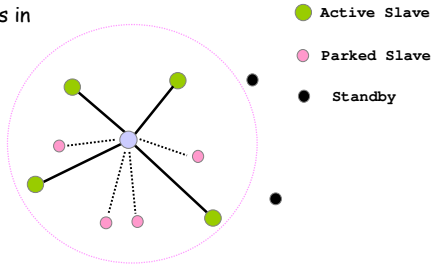


Inquiry on time axis



Piconet formation

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

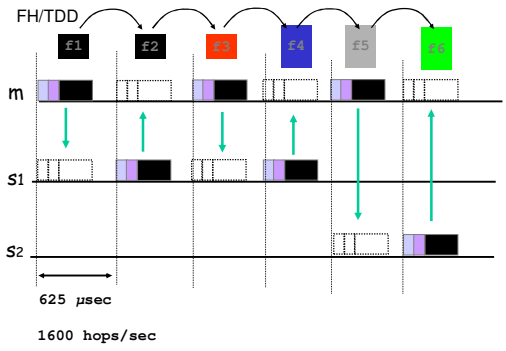


Master
Active Slave
Parked Slave
Standby

Addressing

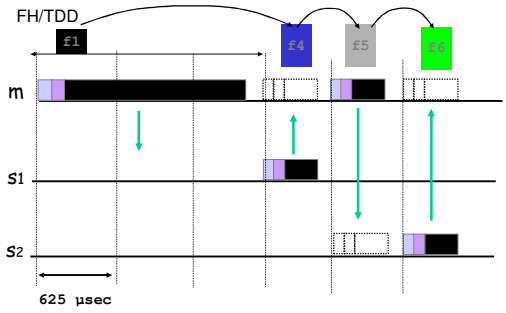
- Bluetooth device address (BD_ADDR)
  - 48 bit IEEE MAC address
- Active Member address (AM_ADDR)
  - 3 bits active slave address
  - all zero broadcast address
- Parked Member address (PM_ADDR)
  - 8 bit parked slave address

Piconet channel



1600 hops/sec

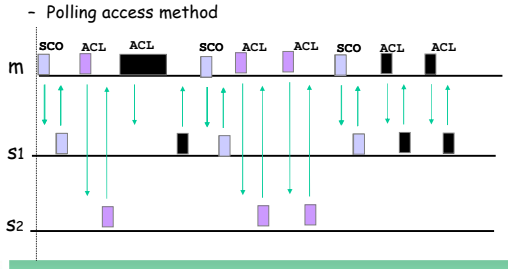
Multi slot packets



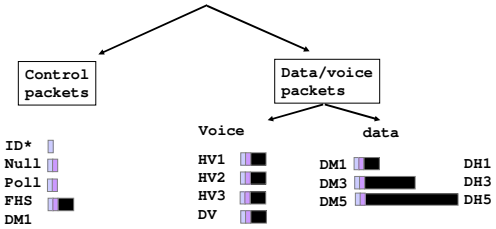
Data rate depends on type of packet

Physical Link Types

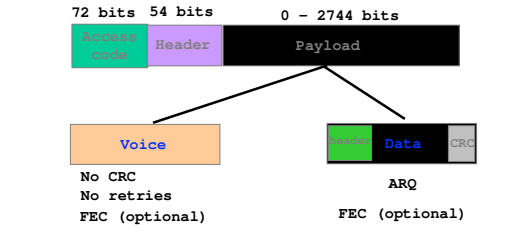
- Synchronous Connection Oriented (SCO) Link
  - slot reservation at fixed intervals
- Asynchronous Connection-less (ACL) Link
  - Polling access method

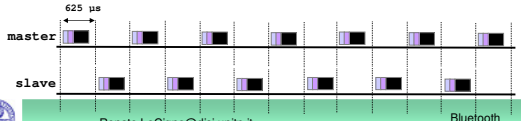


Packet Types

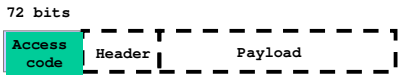


Packet Format





Access Code

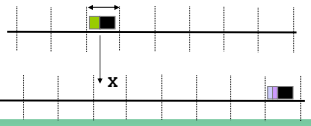


Purpose

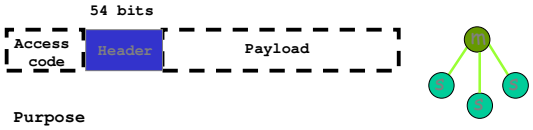
- Synchronization
- DC offset compensation
- Identification
- Signaling

Types

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



Packet Header



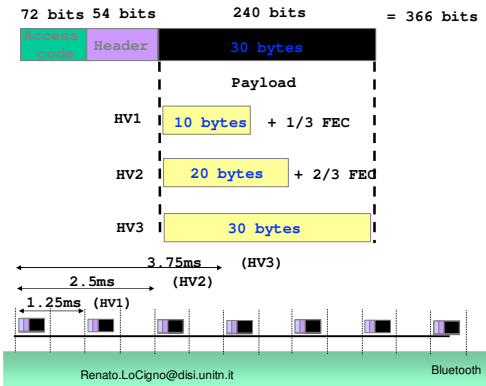
Purpose

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

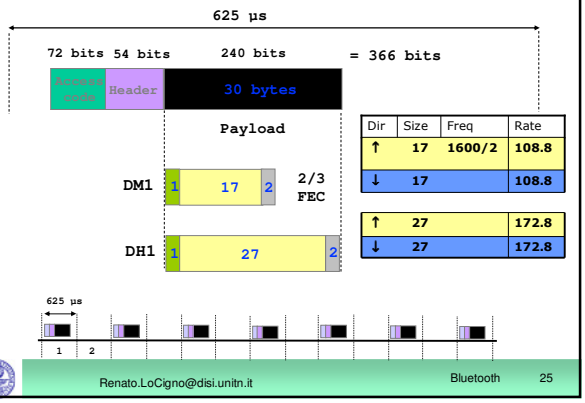
total 18 bits

Encode with 1/3 FEC to get 54 bits

Voice Packets (HV1, HV2, HV3)

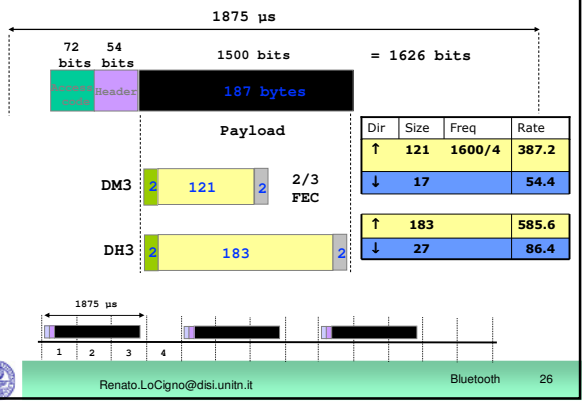


Data rate calculation: DM1 and DH1



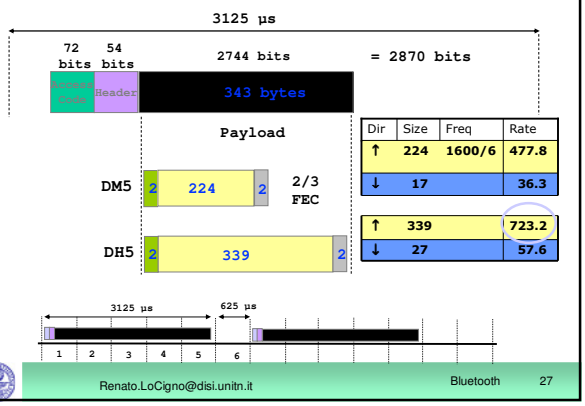
Dir	Size	Freq	Rate
↑	17	1600/2	108.8
↓	17		108.8
↑	27		172.8
↓	27		172.8

Data rate calculation: DM3 and DH3



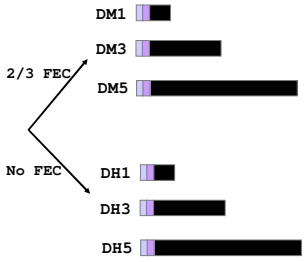
Dir	Size	Freq	Rate
↑	121	1600/4	387.2
↓	17		54.4
↑	183		585.6
↓	27		86.4

Data rate calculation: DM5 and DH5



Dir	Size	Freq	Rate
↑	224	1600/6	477.8
↓	17		36.3
↑	339		723.2
↓	27		57.6

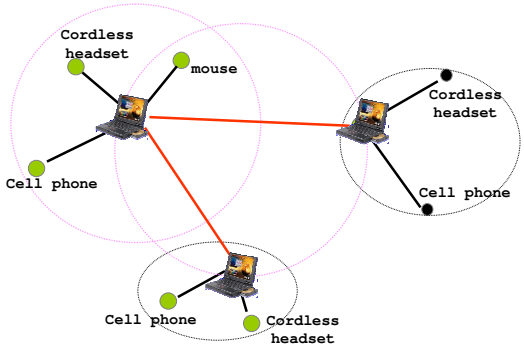
Data Packet Types



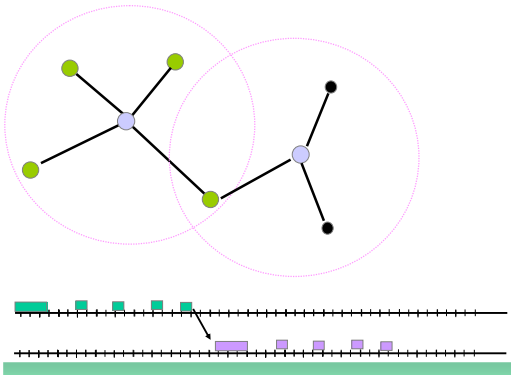
Symmetric	Asymmetric	
108.8	108.8	108.8
258.1	387.2	54.4
286.7	477.8	36.3

Symmetric	Asymmetric	
172.8	172.8	172.8
390.4	585.6	86.4
433.9	723.2	57.6

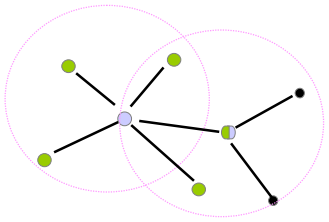
Inter piconet communication



Scatternet



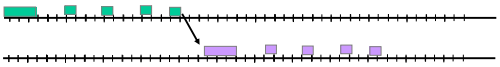
Scatternet, scenario 2



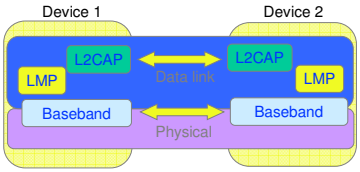
How to schedule presence in two piconets?

Forwarding delay ?

Missed traffic?

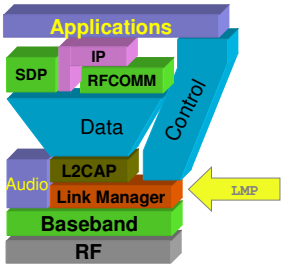


Baseband: Summary



- 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

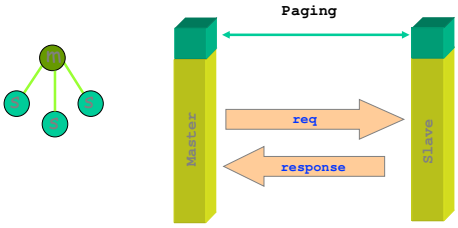


Setup and management of Baseband connections

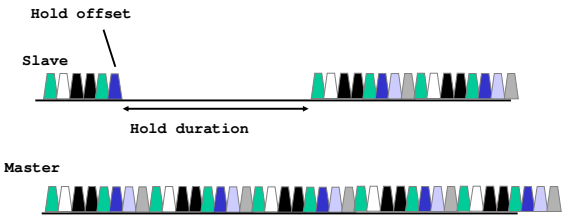
- Piconet Management
- Link Configuration
- Security

Piconet Management

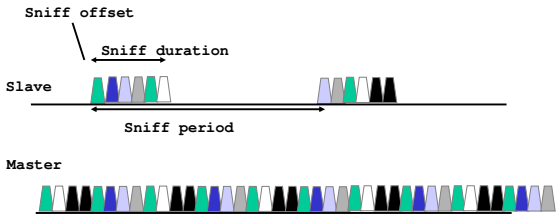
- Attach and detach slaves
- Master-slave switch
- Establishing SCO links
- Handling of low power modes (Sniff, Hold, Park)



Low power mode (hold)

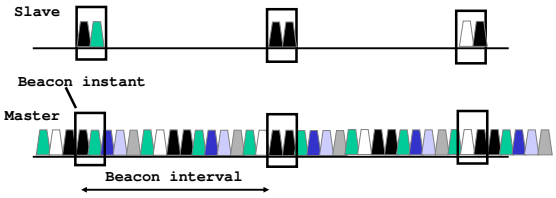


Low power mode (Sniff)



- Traffic reduced to periodic sniff slots

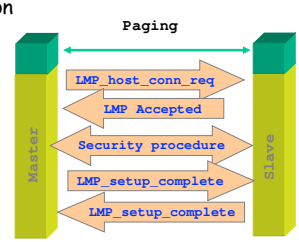
Low power mode (Park)



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

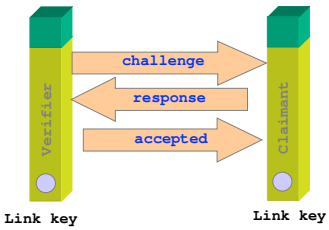
Connection establishment & Security

- 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



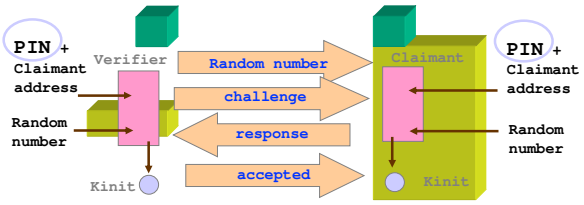
Authentication

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

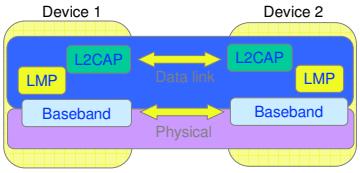


Pairing (key distribution)

- 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

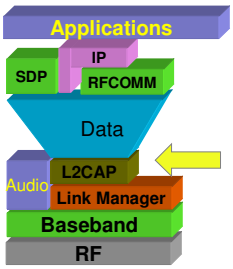


Link Manager Protocol Summary



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

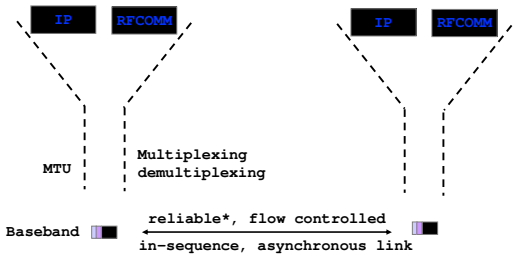
L2CAP



Logical Link Control and Adaptation Protocol

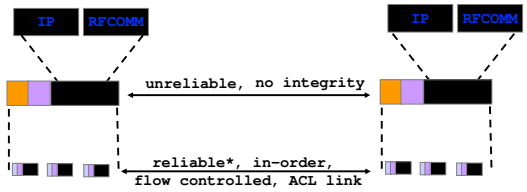
L2CAP provides
- Protocol multiplexing
- Segmentation and Re-assembly
- Quality of service negotiation

Why baseband isn't sufficient



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

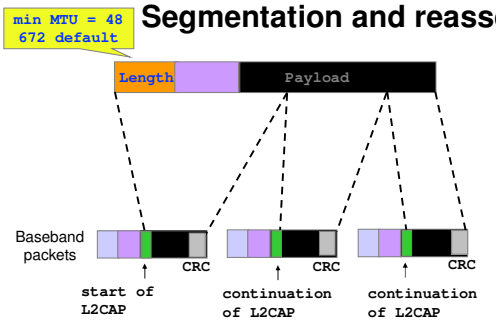
Need a multiprotocol encapsulation layer



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

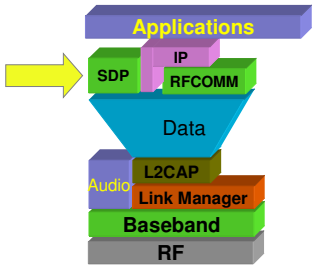
What about
- Reliability?
- Connection oriented or connectionless?
- integrity checks?

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

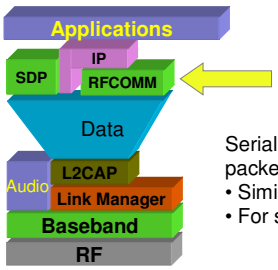
Bluetooth Service Discovery Protocol



Example usage of SDP

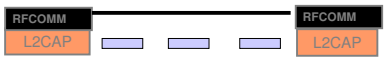
- Establish L2CAP connection to remote device
- Query for services
  - search for specific class of service, or
  - browse for services
- Retrieve attributes that detail how to connect to the service
- Establish a separate (non-SDP) connection to use the service

Serial Port Emulation using RFCOMM



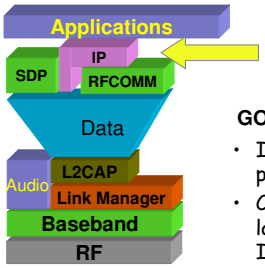
Serial Port emulation on top of a packet oriented link
- Similar to HDLC
- For supporting legacy apps

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

Bluetooth Current Market Outlook

Biggest challenges facing Bluetooth

- Interoperability
  - Always a challenge for any new technology
- Hyped up expectations
- Out of the box ease of use
- Cost target $5
  - well below that
- Critical mass
  - one billion devices sold by Nov.2006
- RF in silicon
- Conflicting interests – business and engineering

Value to carriers: Synchronization and Push

- More bits over the air
- Utilization of unused capacity during non-busy periods
- Higher barrier for switching service providers

Value to carriers: Cell phone as an IP gateway

Will Pilot and cell phone eventually merge?

- More bits over the air
- Enhanced user experience
  - Palmpilot has a better UI than a cell phone
- Growth into other vertical markets

Value to carriers: Call handoff

Threat
or
opportunity?

- More attractive calling plans
- Alleviate system load during peak periods
- Serve more users with fewer resources