BYOES ESC Boston '08:

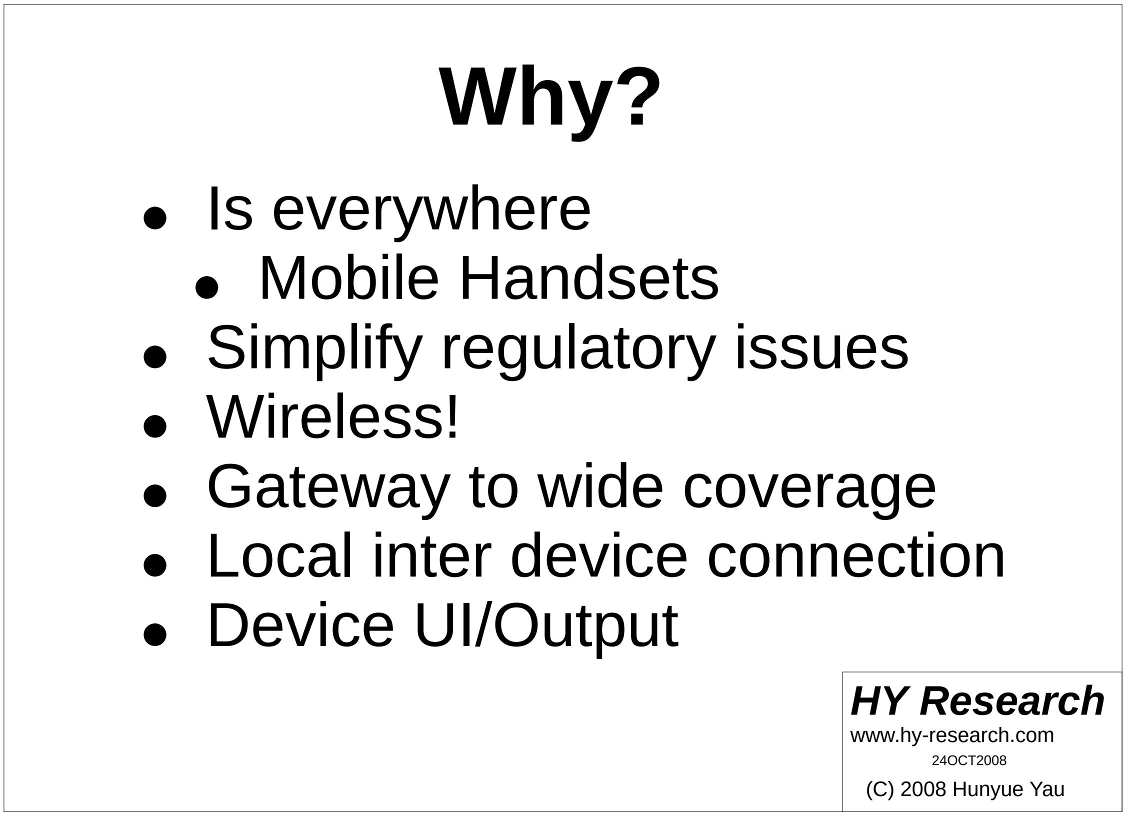
Taking Advantage of Bluetooth®
for Communications and More

by

Hunyue Yau

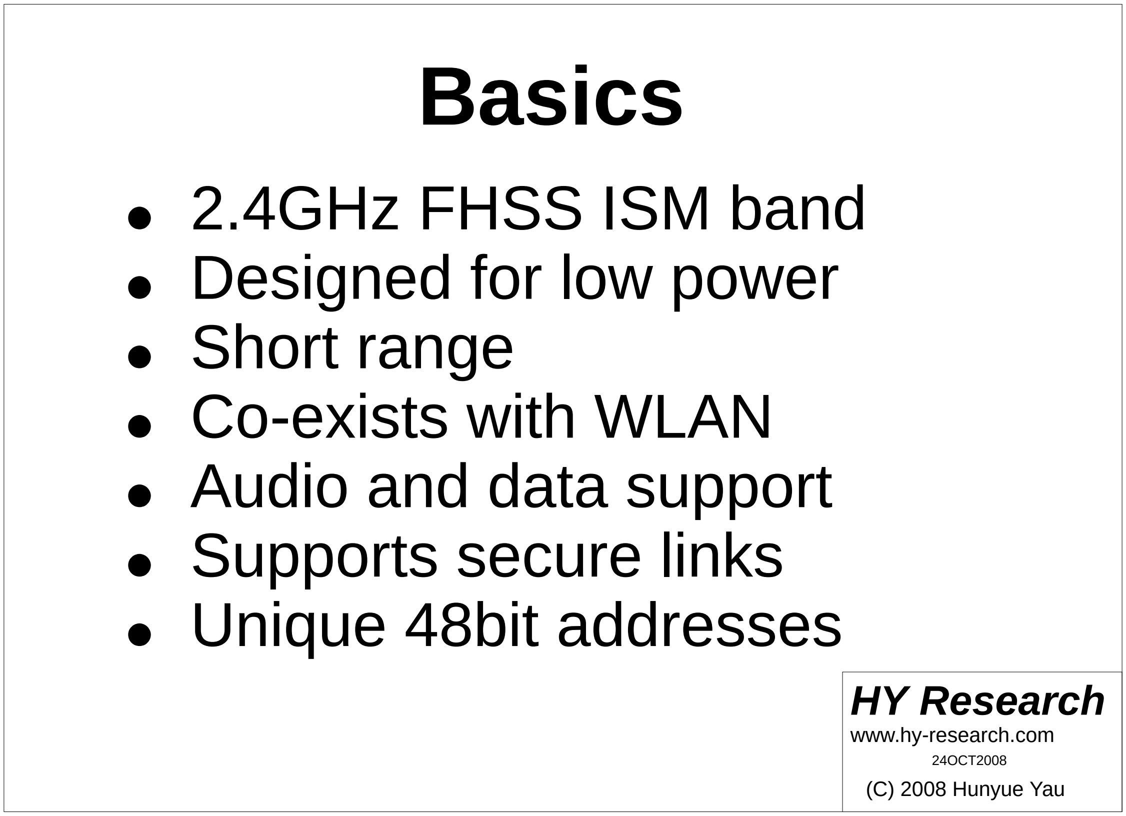
Agenda

- Why?
- Bluetooth®
  - Basics
  - Classes
  - Profiles
  - Service announcement
  - Operation
  - Performance
  - Linux
- Lab



Why?

- Is everywhere
  - Mobile Handsets
- Simplify regulatory issues
- Wireless!
- Gateway to wide coverage
- Local inter device connection
- Device UI/Output



Basics

- 2.4GHz FHSS ISM band
- Designed for low power
- Short range
- Co-exists with WLAN
- Audio and data support
- Supports secure links
- Unique 48bit addresses

Basics (con't)

- Defined by Bluetooth® SIG
  - http://www.bluetooth.org/
- Multiple revisions of the spec.
  - 1.1 improves noise immunity
  - Latest version is 2.1
  - Backward compatible
  - http://www.bluetooth.org/

Classes

- 3 classes defined
- Class 1
  - 100mW (20dBm) about 100M
- Class 2
  - 2.5mW (4dBm) about 10M
- Class 3
  - 1mW (0dBm) about 1M

Profiles

- Defines standard functionalities

  GAP - Generic Access Profile
  DUN - Dial Up Networking Profile
  PAN - Personal Area Network Profile
  HID - Profile
  A2DP - Advance Audio Distribution Profile
  HSP - Head Set Profile
  HFP - Hands Free Profile
  (and more!)

- Can build on top of other profiles

  DUN uses SPP (Serial Port Profile)

Services

- Advertised by a device
- 2 Different means:

  SDAP - Service Discovery Application Profile
  Device class information

- Both/either/neither is required

  Inbound connections may require it
  Outbound connections may not require it

- SDAP may contain other info

Operation

- Pairing

  Synchronization for FHSS
  PIN may be required, sometimes fixed
- Discoverability
- Data rate 723.1Kbits/sec (1.x)
- Data rate 2.1 Mbits/sec (2.x EDR)
- Up to 4 x 64Kbits/sec may be used by SCO audio channels
- Available bandwidth may reduced

Performance

- As little as 500Kbits/sec data

  1.1 device, 4x64K audio active, no environmental factor.
- Context

  EGPRS/EDGE - 474Kbits/sec
  GPRS - 112Kbits/sec
  3G (various) - >1Mbits/sec
- Application dependant

Bluetooth® and Linux

- Bluez software
- Bluez has 2 parts

  Kernel - In Linux 2.6
  Userland - different versions usable
- Hardware supported

  Serial (UART) - includes SDIO and some PCMCIA
  USB
  Chipset specific
- Host Controller Interface
- Data OK with most

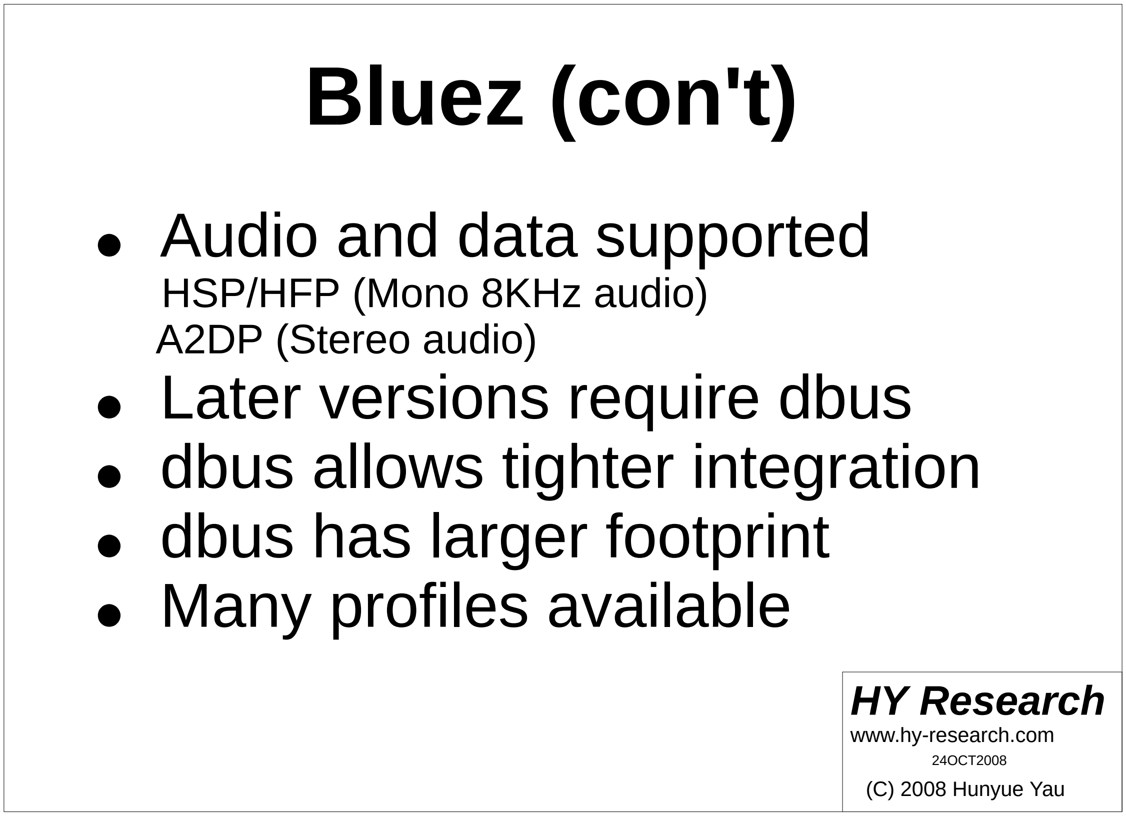
Bluez

- Socket style userland interface
- Devices appear as hciX

```
% hciconfig
hci0: Type: USB
      BD Address: 00:15:83:C2:C3:DD ACL MTU:..
      UP RUNNING PSCAN ISCAN
      RX bytes: 123 acl:0 sco:0 events:30 errors: 0
      TX bytes: 323 acl:0 sco:0 events: 20 errors:0
```

- Utilities

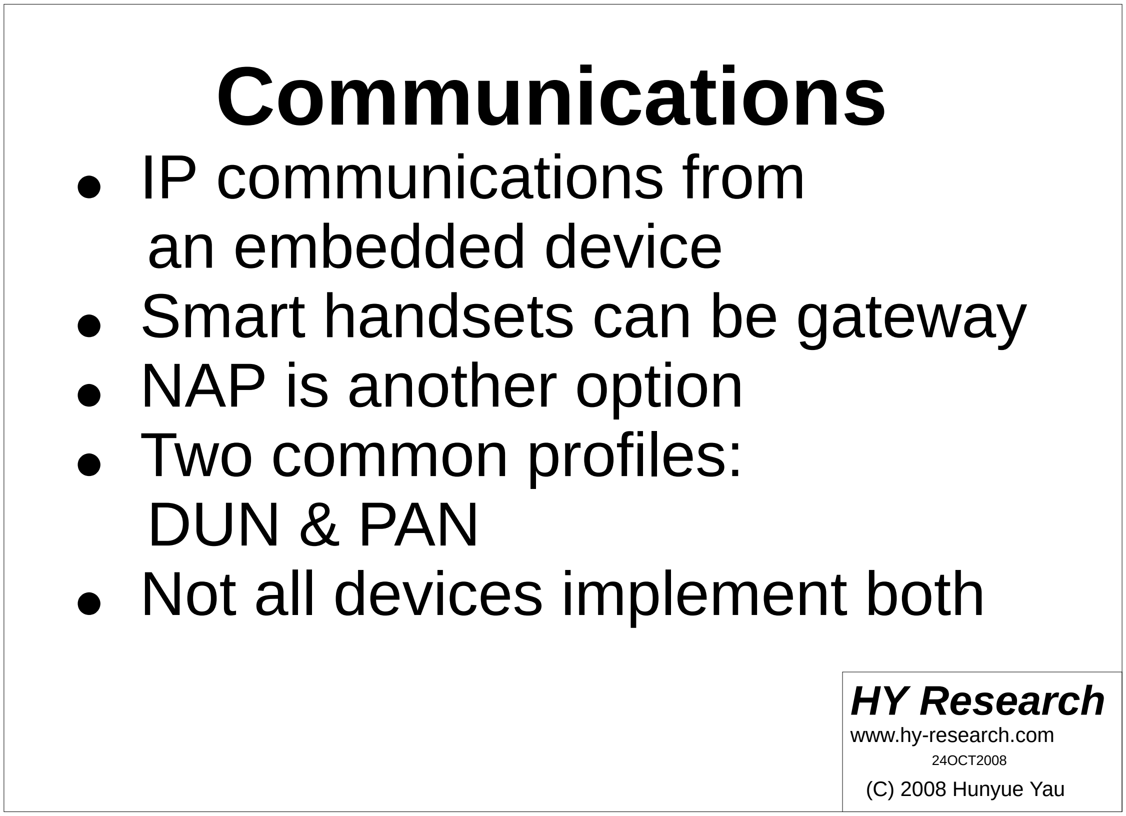
  hcid
  hcitool
  hciconfig
  hciattach (UART devices)
  sdptool



Bluez (con't)

- Audio and data supported
  HSP/HFP (Mono 8KHz audio)
  A2DP (Stereo audio)
- Later versions require dbus
- dbus allows tighter integration
- dbus has larger footprint
- Many profiles available

HY Research
www.hy-research.com
24OCT2008



Communications

- IP communications from
  an embedded device
- Smart handsets can be gateway
- NAP is another option
- Two common profiles:
  DUN & PAN
- Not all devices implement both

HY Research
www.hy-research.com
24OCT2008

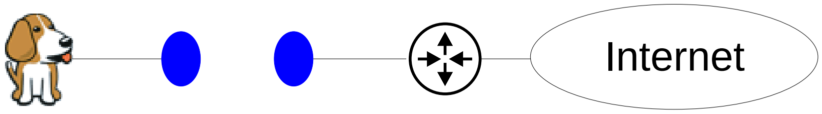
Bluetooth®: DUN

- More common
- Builds on top of SPP
- Like a tethered phone or module
- Reuse wired line modem code
- AT config followed by PPP
- AT commands can vary between provider and device
- rfcomm/dund

Bluetooth®: PAN

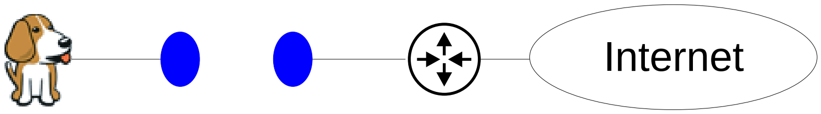
- Less common
- Windows Mobile phones
- Appears as a bnep0 device
- Similar between carriers and devices
- Also used by non Phones
  NAP - Network Access Point
- Use static or DHCP
- pand

BeagleBoard Lab



- Configuration
- Pair with NAP
- Connect to NAP
- Test connection

Lab: Configuration

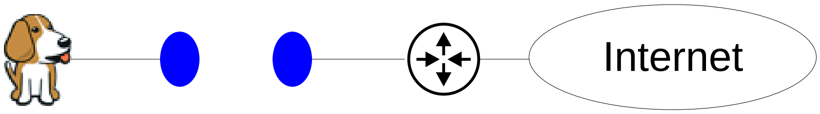


- Configuration defined in /etc/bluetooth/hcid.conf

Lab: hcid.conf

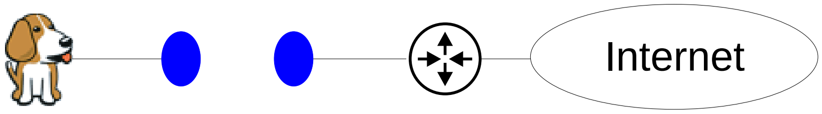
```
options {
    autoinit yes;
    security user;
    pairing multi;
    passkey "0000";
}
device {
    name "BlueZ (%d)";
    class 0x3e0100;
    iscan enable; pscan enable;
    lm accept;
    lp rswitch,hold,sniff,park;
}
```

hcid.conf



- Defines system bluetooth config
- Discoverability
- Service advertisement
- Power management
- Device name

Lab: Pairing



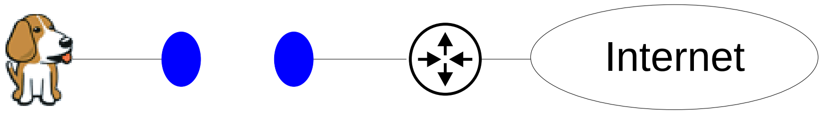
- Discover NAP

```
 % hcitool scan
 Scanning...
       00:11:67:8C:FD:23  Machine
```

- Pair them

```
% hcitool cc 00:11:67:8C:FD:23
```

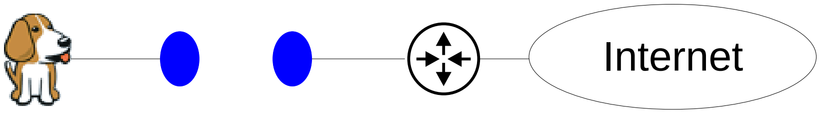
Lab: Pairing



- Examine Peer

```
% hcitool info 00:11:67:8C:FD:23
Requesting information...
   BD Address: 00:11:67:8C:FD:23
   Device Name: TC1000
   LMP Version: 2.0 (0x3) LMP...
   Manufacture: Integrated System...
   ...
```

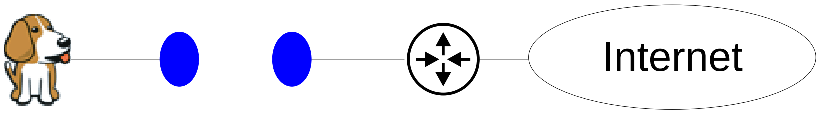
Lab: SDAP



- Browse SDAP offerings

```
% sdptool browse 00:11:67:8C:FD:23
Browsing 00:11:67:8C:FD:23
Service Name: Network Access Point
Service RecHandle: 0x10000
Service Class ID List:
  ....
```

Lab: Connecting



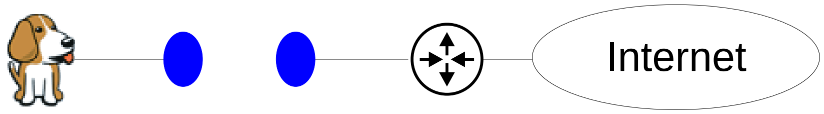
- Run pand

```
% pand -c 00:11:67:8C:FD:23
```

- Show connection

```
% pand -l
 bnep0 00:11:67:8C:FD:23 PANU
```

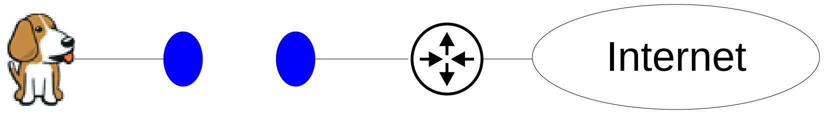
Lab: IP Configuration



- Get IP with DHCP from NAP

```
% dhcpcd bnep0 &
```

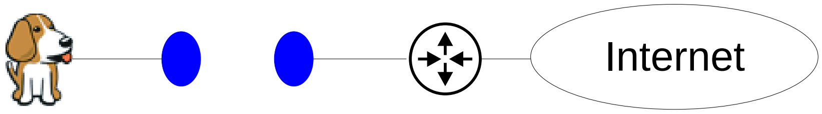
Lab: Verify connection



- Check ifconfig

```
     % /sbin/ifconfig bnep0
bnep0  Link encap:Ethernet HWaddr 00:02:5B:FF:CA:03
       inet addr:172.16.1.20 Bcast:172.16.1.255 Mask:255...
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:134 errors:0 dropped:0 overruns:0 frame:0
       TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
       collisions:54 txqueuelen:100
```

Lab: Send a packet!



- Ping the NAP

```
% ping -c 5 172.17.1.1
PING 172.17.1.1 (172.17.1.1)
64 bytes from 172.17.1.1 icmp_seq=0 ttl=63 time=2.01ms
...
```

- Point browser at
  http://172.17.1.1/

References and Credits

http://www.bluetooth.com/
http://www.bluetooth.org/
http://en.wikipedia.org/wiki/Bluetooth
http://www.bluez.org/
http://www.beagleboard.org/

Beagle Board icon from http://www.beagleboard.org/
Bluetooth® is a registered wordmark of the Bluetooth SIG

Questions?

Slides available at
http://www.hy-research.com/
or email
yesc08@hy-research.com