

SOA-3: Bluetooth™ 101 – Are PANS In Your Future

Bob Brennan
Technical Evangelist
Integrated Manufacturing
Systems, Inc.



Agenda

- Bluetooth Concepts
- Piconet - Hardware Connectivity
- Profiles – Software Capabilities
- Security – Protect Your Stuff
- In Action - Demos



SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Why use Bluetooth®

- Add/Extend Capabilities
- Convenience of the PAN
- New User Paradigm
- Solves a Business Need

SOA-3 Bluetooth 101- Are PANS In Your Future?

3

PROGRESS®
Exchange 08

Who Invented Bluetooth®

- Bluetooth is a trademark owned by Bluetooth SIG, Inc., USA



SOA-3 Bluetooth 101- Are PANS In Your Future?

4

PROGRESS®
Exchange 08

What is Bluetooth®

- Personal Area Networking Technology
- Uses 2.4Ghz Radio Spectrum (ISM)
- Spread Spectrum Frequency Hopping
- “No Wires”
- Single Chip Design
- Platform and Protocol In One Package
- Multiple Capabilities & Profiles

What's With The Name Bluetooth®

- "*Bluetooth*" is from the 10th century Danish King Harald Blatand - or Harold *Bluetooth* in English. King Blatand was instrumental in uniting warring factions in parts of what is now Norway, Sweden and Denmark.
- Think collaboration between differing industries such as the computing, mobile phone and automotive markets.

SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

What?

400

10,000

2,000,000,000



SOA-3 Bluetooth 101- Are PANS In Your Future?

7

PROGRESS
Exchange 08

Agenda

- Bluetooth Concepts
- Piconet - Hardware Connectivity
- Profiles – Software Capabilities
- Security – Protect Your Stuff
- In Action - Demos

SOA-3 Bluetooth 101- Are PANS In Your Future?

8

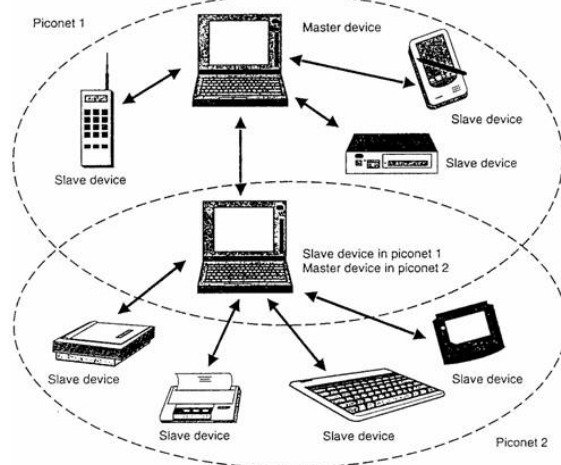
PROGRESS
Exchange 08

Piconet – Hardware Connectivity

- Master/Slave
- Frequency Hopping
- Discovery/Pairing
- Radio Details
- Comparison to other radio technologies



Master Slave Diagram



SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Simplest Form – Piconet

Turn on your
headset

Select the "Add
Bluetooth device"
option on your
phone

Your phone and headset
find each other and
connect automatically

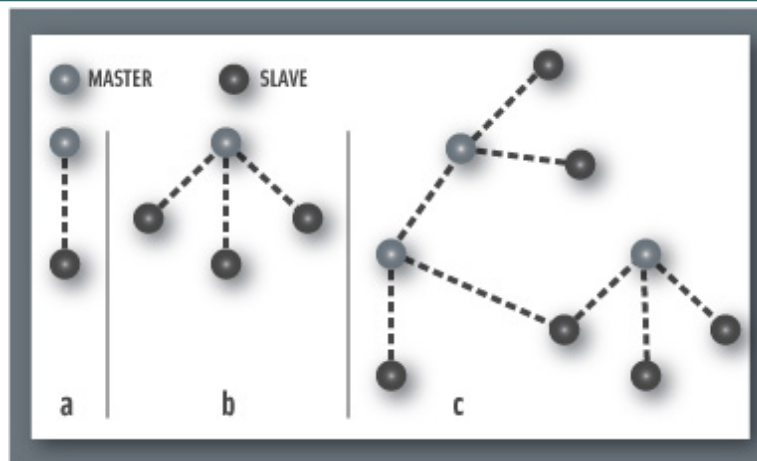


SOA-3 Bluetooth 101- Are PANS In Your Future?

11

PROGRESS
Exchange 08

Piconet & Scatternet



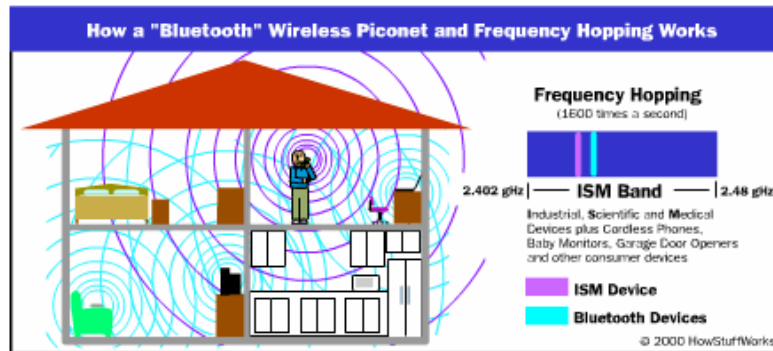
SOA-3 Bluetooth 101- Are PANS In Your Future?

12

PROGRESS
Exchange 08

SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Spread Spectrum Frequency Hopping



1 MHz Jump 1600 Times Per Second

SOA-3 Bluetooth 101- Are PANS In Your Future?

13

PROGRESS
Exchange 08

Discovery - Device Address



- Similar to a MAC addresses on a NIC
- Universally Unique
- Contains identifying information

SOA-3 Bluetooth 101- Are PANS In Your Future?

14

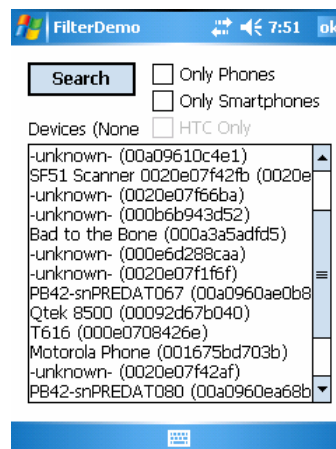
PROGRESS
Exchange 08

Bluetooth Device Address

- Each Bluetooth transceiver is allocated a unique 48-bit device address.
- 24-bit LAP Lower Address Portion
- 16-bit NAP Non-significant Address Portion
- 8-bit UAP Upper Address Portion

Class of Device Filtering

- Not filtered



SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Class of Device Filtering

- Phones Filter

The screenshot shows a window titled "FilterDemo" with a status bar at the top displaying signal strength, volume, and time (7:51). Below the title bar is a "Search" button and three checkboxes: "Only Phones" (checked), "Only Smartphones" (unchecked), and "HTC Only" (unchecked). Under the "Phones" label, a list box contains three entries: "Qtek 8500 (00092d67b040)", "T616 (000e0708426e)", and "Motorola Phone (001675bd703b)". At the bottom of the window is a blue bar with a small icon.

SOA-3 Bluetooth 101- Are PANS In Your Future?

17

PROGRESS
Exchange 08

Needle in the Haystack

- Smart Phone Filter

The screenshot shows the same "FilterDemo" window. The "Only Smartphones" checkbox is now checked, and the "Only Phones" checkbox remains checked. The list box under the "SmartPhones" label now contains only one entry: "Qtek 8500 (00092d67b040)". The "HTC Only" checkbox remains unchecked. The rest of the window interface is identical to the previous slide.

SOA-3 Bluetooth 101- Are PANS In Your Future?

18

PROGRESS
Exchange 08

SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Device Address Components



NAP LAP
00092D67B040
UAP

NAP + UAP = Vendor

0009 + 2D = HTC, Inc.

On Demand Broadcast

- Device name
- Device class
- List of services
- Technical information, for example, device features, manufacturer, Bluetooth specification used, clock offset



Class Of Device

- Identifying number allowing devices to announce themselves as computers, phones, printers, etc.
- Service type information is also included
- Mobile Phone Examples
 - 52020c - Blackjack
 - 522204 - RAZR
 - 50020c – Qtek 8500

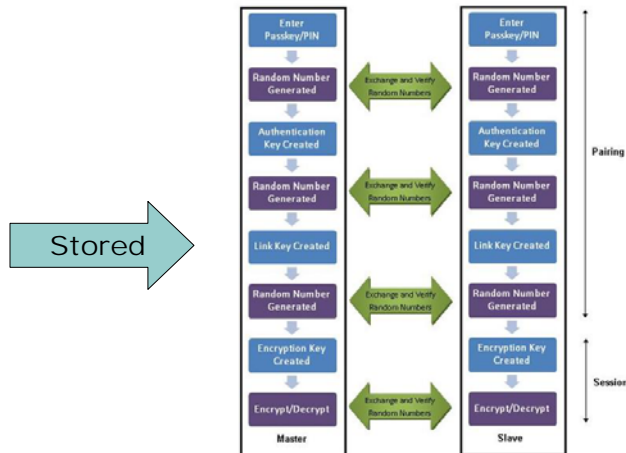
Pairing

- Bluetooth pairing occurs when two Bluetooth devices agree to communicate with each other and establish a connection.



SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Pairing



SOA-3 Bluetooth 101- Are PANS In Your Future?

23

PROGRESS
Exchange 08

Radio Characteristics

ISM Band 2.45 GHz (2.402 – 2.480 GHz)

79 individual 1 MHz Frequencies

1 Milliwatt radio → Very Low Power

Low Power → Longer Battery Life



SOA-3 Bluetooth 101- Are PANS In Your Future?

24

PROGRESS
Exchange 08

SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Comparison Of PAN Technologies

Features	Bluetooth	IrDA	UWB	ZigBee
Rate	720 kbps to 3 Mbps	4 Mbps (max)	480 Mbps	20 kbps
Line of Sight	No	Yes	No	No
Range	1 to 100 m	1 m	10 m and above	10 to 100 m
Power	Low	Moderate	Low	Ultra-low
Cost	Low	Ultra-Low	Medium	Ultra-low

IrDA – Infrared

UWB - Ultra Wide Band - Defunct

SOA-3 Bluetooth 101- Are PANS In Your Future?

25

PROGRESS
Exchange 08

Agenda

- Bluetooth Concepts
- Piconet - Hardware Connectivity
- Profiles – Software Capabilities
- Security – Protect Your Stuff
- In Action - Demos

SOA-3 Bluetooth 101- Are PANS In Your Future?

26

PROGRESS
Exchange 08

Profiles

- General behaviors through which *BT* enabled devices communicate.
- Protocol for interaction between the master & slave
- 25+ Unique Profiles & Protocols

Profiles

- List of various Capabilities & Protocols
- Both Master and Slave Must Implement a Profile for It To Be Used
- Interest to the Business App Developer
- “BT is not a solution without software”

All Current Profiles

- Details provided on the CD
- http://en.wikipedia.org/wiki/Bluetooth_profile



Interesting Profiles

Dial-Up Network (DUN)

Access the Internet and other dial-up services

Human Interface Device (HID)

Protocols, procedures and features to be used by *BT* HID such as keyboards, pointing devices, and remote monitoring devices.

Object Exchange (OBEX)

Data objects and a communication protocol two devices can use to exchange those objects

Agenda

- Bluetooth Concepts
- Piconet - Hardware Connectivity
- Profiles – Software Capabilities
- Security – Protect Your Stuff
- In Action - Demos

Pairing & Security

- Bluetooth implements
 - Confidentiality
 - Authentication
 - Key derivation with custom algorithms based on the SAFER+ block cipher.
- PIN or Key Code on Master & Slave

Security Concerns

- Device Discoverable?
- Positive ID On Devices
- Predictable & Weak Pass Keys
- Social Engineering the Neophytes



Modes Of Security

- Non Secure
- Service Level Security
- Link Level Security



SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Re-Cap Bluetooth®

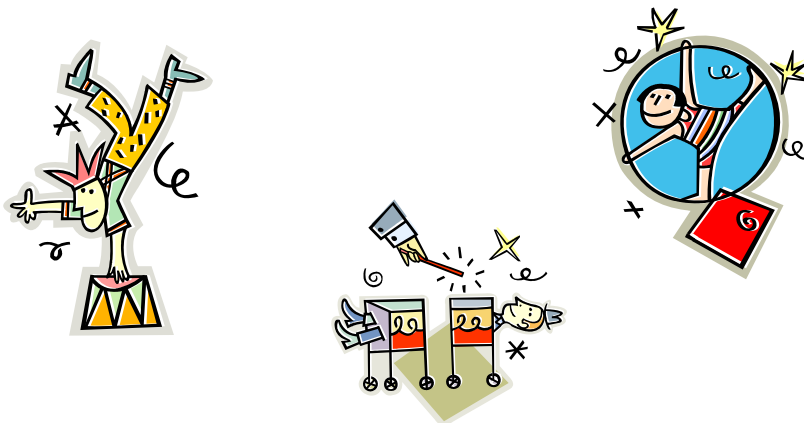
- Personal Area Network Protocol
- Master Slave Topology
- Profiles
- Secure Communications

SOA-3 Bluetooth 101- Are PANS In Your Future?

35

PROGRESS
Exchange 08

Demos



SOA-3 Bluetooth 101- Are PANS In Your Future?

36

PROGRESS
Exchange 08

SOA-3: Bluetooth 101- Are PANS In Your Future?
Bob Brennan

Suggested Reading

<http://www.bluetooth.com>

<http://electronics.howstuffworks.com/bluetooth.htm>

http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security_Paper.pdf

SOA-3 Bluetooth 101- Are PANS In Your Future?

37

PROGRESS
Exchange 08

Questions/Comments/Discussion

Thank You for Attending

Bob Brennan
Integrated Manufacturing Systems, Inc.
(603) 424-0109

SOA-3 Bluetooth 101- Are PANS In Your Future?

38

PROGRESS
Exchange 08