By Sailesh Rathi,
Microware Architect,
Microware Systems Corporation.

Blue Tooth Protocol Architecture

Bluetooth is an open specification for a radio system that provides the network infrastructure to enable short range wireless communication of data and voice. It comprises of a hardware component and a software component. The specification also describes usage models and user profiles for these models. Bluetooth is named after the Danish King Harald Blaatand. This article gives you an overview of the Protocol architecture.

WHAT IS BLUETOOTH?

Bluetooth is an open specification for a radio system that provides the network infrastructure to enable short range wireless communication of data and voice. It comprises of a hardware component and a software component. The specification also describes usage models and user profiles for these models. Bluetooth is named after the Danish King Harald Blaatand "Bluetooth", who successfully united Denmark and Norway during his rule from 940 to 985 AD.

Bluetooth unleashes the concept of "hidden computing" by providing radio devices "unconscious" connectivity without the user's proactive intervention. It provides a bearer service for wireless (WAP) applications.

BLUETOOTH CHARACTERISTICS

Bluetooth radios operate in the unlicensed ISM band at 2.4 Gigahertz using 79 channels between 2.402 GHz to 2.480 GHz (23 channels in some countries). The range for bluetooth communication is 0-30 feet (10 meters) with a power consumption of 0dBm (1mW). This distance can be increased to 100 meters by amplifying the power to 20dBm. The bluetooth radio system is optimized for mobility.

Bluetooth supports two kinds of links: Asynchronous Connectionless (ACL) links for data transmission and Synchronous Connection oriented (SCO) links for audio/voice transmission. The gross bluetooth data rate is 1 Mbps while the maximum effective rate on an asymmetric ACL link is 721 Kbps in either direction and 57.6 Kbps in the return direction. A symmetric ACL link allows data rates of 432.6 Kbps. Bluetooth also supports up to three 64Kbps SCO channels per device. These channels are guaranteed bandwidth for transmission.

TECHNOLOGY COMPARISON

Since bluetooth operates in the unlicensed ISM band that is also used by other devices such as 802.11 networks, baby monitors, garage door openers, microwave ovens etc, there is possibility of interference. Bluetooth uses Frequency Hop Spread Spectrum (FHSS) to avoid any interference. A bluetooth channel is divided into time slots each 625 micro second in length. The devices hop through these timeslots making 1600 hops per second. This trades bandwidth efficiency for reliability, integrity and security.

BLUETOOTH ARCHITECTURE

Bluetooth communication occurs between a master radio and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also the slave. Each radio has a 48 bit unique device address (BD_ADDR) that is fixed.

Two or more radio devices together form ad-hoc networks called piconets. All units within a piconet share the same channel. Each piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a piconet. Thus each active device within a piconet is identifiable by a

Category	Home-RF (1.09)	802.11	Bluetooth	IrDA (AIR)
Market	Home WLAN	WLAN	Cable	Cable
Technology	RF: 2.4 GHz FHSS	RF: 2.4 GHz FHSS/DSSS	RF: 2.4 GHz FHSS	Optical 850 nm
Power	20dBm	20dBm	0/20dBm	?
Symbol Rate	0.8/1.6 M	11M	1M	4M/115K
Distance	50m	30-100 m	0-10m/100 m	0-3m/5m
Topology	128 devices CSMA	128 devices CSMA	8 devices Pt to MP	10 devices Pt to MP
Security	Optional	Optional WEP	Authentication, Key, mgmt, Encryption	Application Layer
Cost	Low	High	Low	Low

Figure 1. Technology comparison.

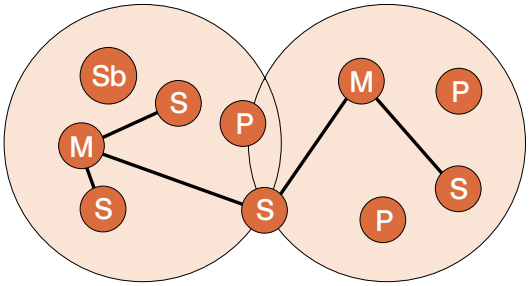

Figure 2. A Scatternet comprising two Piconets.

3 bit active device address. Inactive slaves in unconnected modes may continue to reside within the piconet.

A master is the only one that may initiate a bluetooth communication link. However, once a link is established, the slave may request a master/slave switch to become the master. Slaves are not allowed to talk to each other directly. All communication occurs within the slave and the master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master. Each piconet uses a different frequency hopping sequence. Radio devices used Time Division Multiplexing (TDM). A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

Multiple piconets with overlapping coverage areas form a scatternet. Each piconet may have only one master, but slaves may participate in different piconets on a time-division multiplex basis. A device may be a master in one piconet and a slave in another or a slave in more than one piconet.

Bluetooth Core Protocols	Baseband, LMP, L2CAP, SDP
Cable Replacement Protocol	RFCOMM
Telephony Control Protocol	TCS Binary, AT Commands
Adopted Protocols	PPP, TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE

THE PROTOCOL STACK

The protocols of the bluetooth stack can be divided into four different categories:

BLUETOOTH CORE PROTOCOLS

BaseBand

The baseband and the Link control layers enable the physical RF link between bluetooth devices to form a piconet. Both circuit and packet switching is used. They provide two kinds of physical links using the baseband packets. Synchronous connection oriented (SCO) and Asynchronous connectionless (ACL). ACL packets are used for data only, while the SCO packets may contain audio only or a combination of audio and data.

The Link Manager Protocol

The link manager protocol is responsible for the link setup between bluetooth units. This protocol layer caters to issues of security like authentication, encryption by generating, exchanging and checking the link and encryption keys. It also deals with control and

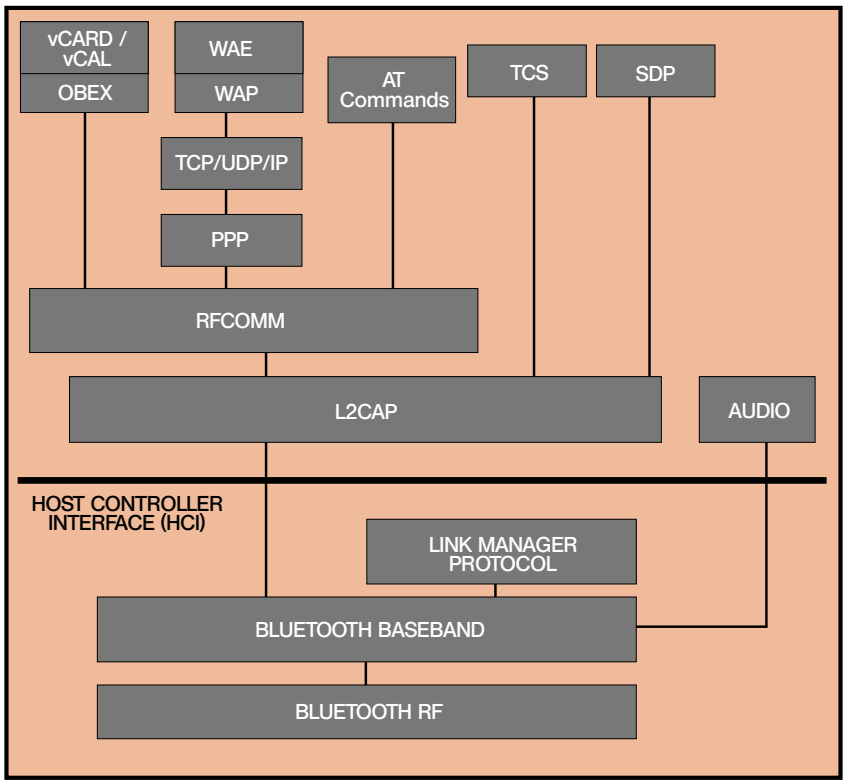

Figure 3. The Bluetooth Protocol Stack.

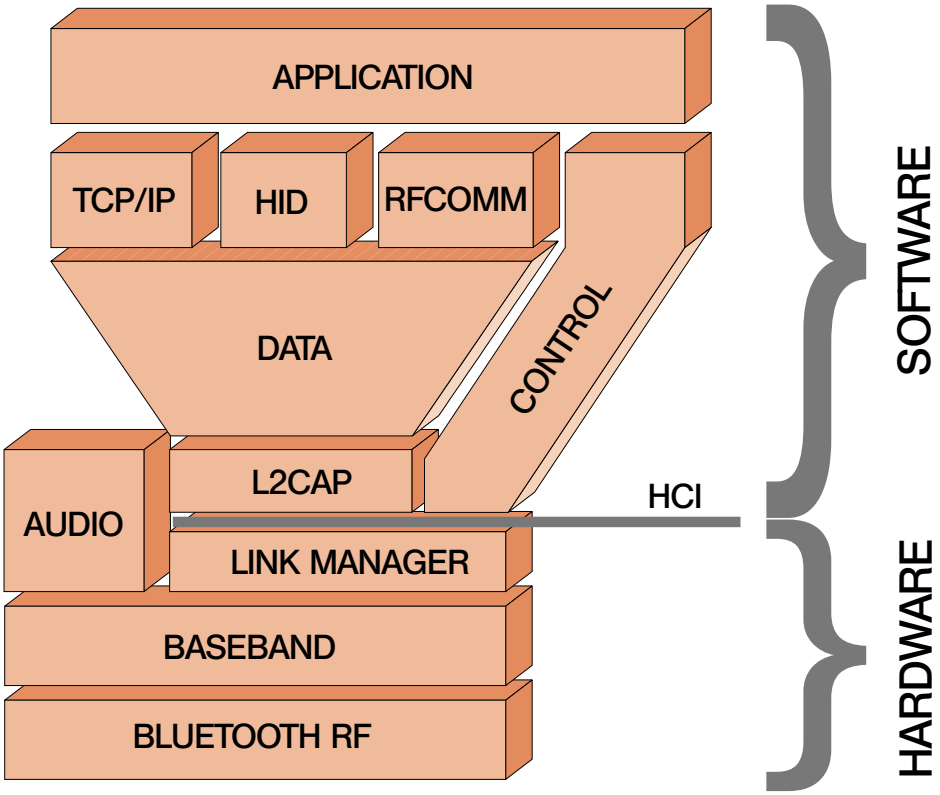

Figure 4. Core protocols.

negotiation of baseband packet sizes.

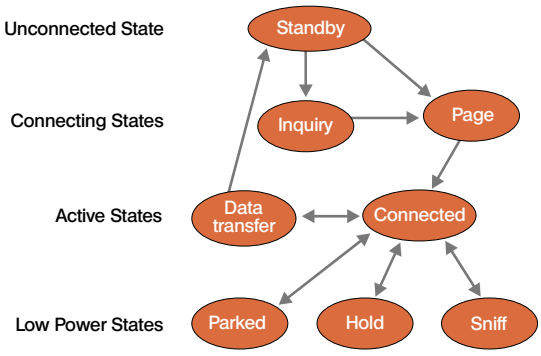

Figure 5. The Baseband State Machine.

Logical Link Control and Adaptation Layer (L2CAP)

The bluetooth logical link control and adaptation layer supports higher level multiplexing, segmentation and reassembly of packets, and Quality of Service (QoS) communication and Groups. This layer does not provide any reliability and uses the baseband ARQ to ensure reliability. Channel identifiers are used to label each connection end point.

Service Discovery Protocol (SDP)

SDP is the basis for discovery of services on all bluetooth devices. This is essential for all bluetooth models. Using the SDP device information, services and the characteristics of the services can be queried and after that a connection between two or more bluetooth devices may be established. Other service discovery protocols such as Jini, UpnP etc. maybe used in conjunction with the bluetooth SDP protocol.

RFCOMM

The RFCOMM protocol is the basis for the cable replacement usage of bluetooth. It is a simple transport protocol with additional provisions for emulating the 9 circuits of RS-232 serial ports over L2CAP part of the bluetooth protocol stack. This is based in the ETSI standard TS 07.10 and supports a large base of legacy applications that use serial communication. It provides a reliable data stream, multiple concurrent connections, flow control and serial cable line settings.

Telephony Control Protocol Specification (TCS Binary)

The TCS binary protocol defines the call control signaling for the establishment of speech and data calls between bluetooth devices. It is based on the ITU-T Q.931 recommendation. It is a bit oriented protocol and also provides group management.

The Host Controller Interface (HCI)

The HCI provides a command interface to the base-

AD RTS PARIS

band controller, link manager and access to the hardware status and control registers. The interface provides a uniform method of accessing the bluetooth baseband capabilities. The Host control transport layer abstracts away transport dependencies and provides a common device driver interface to various interfaces. Three interfaces are defined in the core specification: USB, RS-232, and UART.

ADOPTED PROTOCOLS

PPP, TCP/IP

PPP, TCP, UDP and IP are standard Internet protocols defined by IETF. These are used as the lower layer protocols of the WAP stack.

OBEX

OBEX is a session protocol defined by IrDA. This protocol is also utilized by bluetooth thus enabling the possibility for application to use either the bluetooth radio or IrDA technologies.

WAP/WAE

Bluetooth may be used as a bearer technology for transporting between a WAP client and a nearby WAP server. WAP operates on top of the bluetooth stack using PPP and the TCP/IP protocol suite.

BLUETOOTH USAGE MODELS

Usage models are scenarios that the user may encounter in their personal connectivity bubble and that can be resolved using bluetooth. Usage models provide a means of marketing input into the development process to solve real customer needs.

BLUETOOTH PROFILES

Profiles represent default solutions for usage models. They may be thought of as a vertical slice through the protocol stack. They define the protocols and the protocol features supporting a usage model. These profiles are the basis for interoperability and bluetooth logo requirements. Each bluetooth device supports one or more profiles. There are four generic profiles that are used by the different usage model based profiles. These are serial port profile, generic access profile, Service discovery application profile and generic object exchange profile.

Specification and Description Language (SDL) is an object-oriented, formal language defined by ITU-T as recommendation Z.100. The language is intended for specification of complex, event driven real-time, and interactive applications involving concurrent activities that communicate using discrete signals.

BLUETOOTH PACKET FORMATS

BASEBAND

Access code	Packet header	Payload
72 bits	54 bits	0-2754 bits

L2CAP

Connection Oriented

Length	DCID	Payload
16 bits	16 bits	0-65535 bits

Connection Less Data

Length	DCID	PSM	Payload
16 bits	16 bits	16 bits	0-65533 bits

Signaling Packet

Length	DCID	Code	ID	Length	Payload
16 bits	16 bits	8 bit	8 bit	16 bits	0-65531 bits

DCID: Destination Channel ID

L2CAP	L2CAP multiplexes protocols and performs segmentation/ reassembly for a Bluetooth link connection.
RFCOMM	RFCOMM is a serial port data and flow control emulator.
Service Discovery Protocol (SDP)	The Service Discovery Protocol provides a database of device services.
Management Entity (ME)	Management Entity provides integrated control of the link manager and baseband layers for connections, authentication, encryption, and slave modes.
Multi-transport Object Exchange (OBEX) API	The OBEX component allows applications to send and receive business cards, files, PIM data, and other objects using the OBEX protocol. It supports multiple lower-layer transports including Bluetooth, IrDA and TCP/IP.
HCI Transport Drivers	Portable HCI parser and UART transport code allows the stack to use any HCI-compliant Bluetooth hardware over a UART serial connection. A sample UART driver is provided.
TCS Binary	TCS Binary allows sophisticated control of calls between Bluetooth-enabled phones and gateways.
Voice/Audio	Voice/Audio components allow full-duplex conversations and audio feedback.
Sample Applications	Sample applications show how to use stack components to establish connections, perform inquiries, and exchange data.

Figure 6. The OS-9 Bluetooth Components.

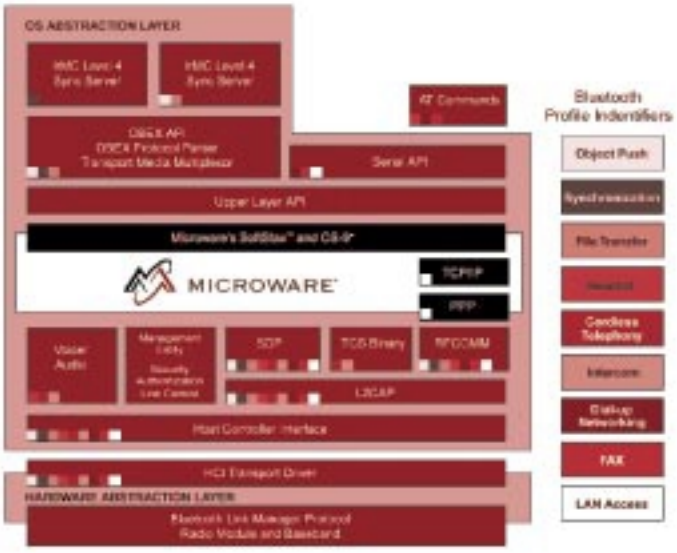

Figure 7. The OS-9 Bluetooth Protocol Stack.

- 0x0002: Connectionless data connection.
- 0x0001: L2CAP signaling packet.

THE OS-9® BLUETOOTH STACK

The OS-9® bluetooth stack is based on the Extended Systems XTNDAccess® Blue SDK 1.1.1. It is built within the SoftStax® network framework. It has an abstraction layer for the bluetooth hardware and comprises of HCI transport driver for UART, RS-232 and USB. The protocol stack is approximately 60K in size. It contains a multi-transport OBEX protocol that is IrMC level 4 capable. The color coding in the above block diagram associates the profiles and the protocols needed to support that profile. For example IrMC is a component of only the synchronization profile while the L2CAP protocol is part of all the profiles.

The OS-9 solution supports all the profiles defined by the Bluetooth Special Interest Group (SIG). The following table lists the different components of the OS-9 stack.

XTNDAccess® Blue SDK 1.1.1 is certified on the Bluetooth Qualified Product list (BQPL) along with the following profiles: Object Push, File Transfer, Dial-up Networking, LAN Access, FAX, Cordless Telephony, Headset, Intercom, Serial Port, L2CAP (Protocol), Service Discovery Protocol (SDP), General Object Exchange Profile (GOEP), and Generic Access (GAP) profiles.

BLUETOOTH AND IEEE 802.15 STANDARD

IEEE has a number of network standards in the 802-series, including 802.3 (Ethernet) and 802.11 (wireless LAN). The latest member of the 802 family, Wireless Personal Area Network (WPAN), is a network paradigm addressing the needs of an inexpensive, short range, low power communications protocol. A WPAN is defined as a ten meter personal connectivity bubble. This bubble comprises of wireless devices which talk the WPAN protocol. The bluetooth protocol is being considered by the 802.15 WPAN standards task group. The 802.15 task group has decided that the standard would be defines in SDL.

ABBREVIATIONS AND ACRONYMS

- ACL: Asynchronous Connectionless
- ETSI: European Telecommunications Standardization Institute
- HCI: Host Controller Interface
- GAP: Generic Access Profile
- IrMC: Infrared Mobile Communication Standard
- ITU: International Telecommunication Union
- ITU-T Q.931: ITU-T Recommendation "Digital subscriber Signaling System No. 1 (DSS 1) - ISDN user-network interface layer 3 specification for basic call control
- L2CAP: Logical Link Control and Adaptation Layer
- LMP: Link Manager Protocol
- ME: Management Entity
- OBEX: Object Exchange Standard
- PSM: Protocol and Service Multiplexer
- QoS: Quality of Service
- RFCOMM: Radio Frequency Communication Protocol
- SCO: Synchronous Connection Oriented
- SDL: Specification and Description Language
- SDP: Service Discovery Protocol
- TCS: Telephony Control Protocol Specification
- TS 07.10: ETSI Technical Specification Standard
- vCard, vCal: IrDa based Applications
- WAE: Wireless Application Environment
- WAP: Wireless Application Protocol
- WEP: Wireless Encryption Protocol
- WPAN: Wireless Personal Area Network ■

Sailesh Rathi is a Software Architect for Microware Systems Corporation. Sailesh has a MBA from Iowa State University, an MS in Computer Science from Loyola University, and a BS in Computer Science and Engineering from Jadavpur University, India. With over seven years of networking and embedded systems experience, Sailesh also designed and implemented the company's IEEE 1394 solution. Sailesh was also involved in the company's implementation of an IEEE 802.11.