# Bluetooth Tutorial

Bluetooth strives to remove the never ending maze of wires which provide a communication link between different electronic devices, through a short range wireless solution. Consider the possibilities: connecting different parts of a computer (eg. keyboard, mouse, printer) without wires, a mobile phone handsfree without the wired link to the mobile, seamlessly synchronizing personal information (like calendars, address book etc.) between a cellphone, laptop and desktops.

# Bluetooth Introduction

Bluetooth is the name given to a new technology standard using short-range radio links, intended to replace the cable(s) connecting portable and/or fixed electronic devices. The standard defines a uniform structure for a wide range of devices to communicate with each other, with minimal user effort.

Its key features are robustness, low complexity, low power and low cost. The technology also offers wireless access to LANs, PSTN, the mobile phone network and the Internet for a host of home appliances and portable handheld interfaces.

The immediate need for Bluetooth came from the desire to connect peripherals and devices without cables. The available technology-IrDA OBEX (IR Data Association Object Exchange Protocol) is based in IR links that are limited to line of sight connections. Bluetooth integration is further fueled by the demand for mobile and wireless access to LANs, Internet over mobile and other existing networks, where the backbone is wired but the interface is free to move. This not only makes the network easier to use but also extends its reach. The advantages and rapid proliferation of LANs suggest that setting up personal area networks, that is, connections among devices in the proximity of the user, will have many beneficial uses.

Bluetooth could also be used in home networking applications. With increasing numbers of homes having multiple PCs, the need for networks that are simple to install and maintain, is growing. There is also the commercial need to provide "information push" capabilities, which is important for handheld and other such mobile devices and this has been partially incorporated in Bluetooth. Bluetooth’s main strength is its ability to simultaneously handle both data and voice transmissions, allowing such innovative solutions as a mobile hands-free headset for voice calls, print to fax capability, and automatically synchronizing PDA, laptop, and cell phone address book applications.

These uses suggest that a technology like Bluetooth is extremely useful and will have a significant effect on the way information is accessed and used.

# Bluetooth Technology

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 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) (Bluetooth Protocol Architecture, White Paper). 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.

# 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 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.

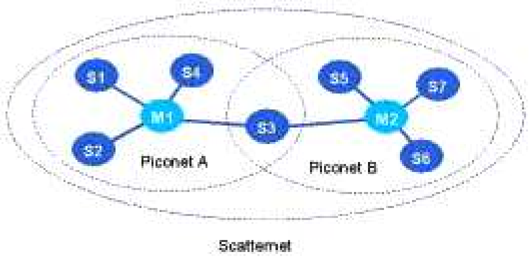

*Fig 1: Bluetooth Scatternets and Piconets*

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.

# Protocol Stack

The Bluetooth Special Interest Group (SIG) has developed the Bluetooth Protocol Stack. These specifications allow for developing interactive services and applications over interoperable radio modules and data communication protocols. Given below is an overview of the protocols in the specification.

The main objective of these specifications is to set down the protocols that must be followed by companies when manufacturing and developing both software and hardware to interoperate with each other. To achieve this interoperability, matching applications (e.g., corresponding client and server application) in remote devices must run over identical protocol stacks.

Different applications may run over different protocol stacks however they will all have one imperative factor that will allow them to be interoperable and that will be the use of a common Bluetooth data link and physical layer. The complete Bluetooth protocol stack is shown in figure below. It may seem that an application must use all protocols shown however not all applications will make use of all the protocols shown. Instead, applications run over one or more vertical slices from this protocol stack.

The main principle in mind when developing the Bluetooth Protocol Architecture has been the maximization and the re-use of existing protocols for different purposes at the higher layers. The one main advantage is that existing (legacy) applications can be adapted to work with the Bluetooth Technology. The Bluetooth Protocol Architecture also allows for the use of commonly used application protocols on top of the Bluetooth-Specific protocols. In simpler terms, this permits new applications to take full advantage of the capabilities of the Bluetooth technology and for many applications that are already developed by vendors; they can take immediate advantage of hardware and software systems, which are also compliant with the Specification.

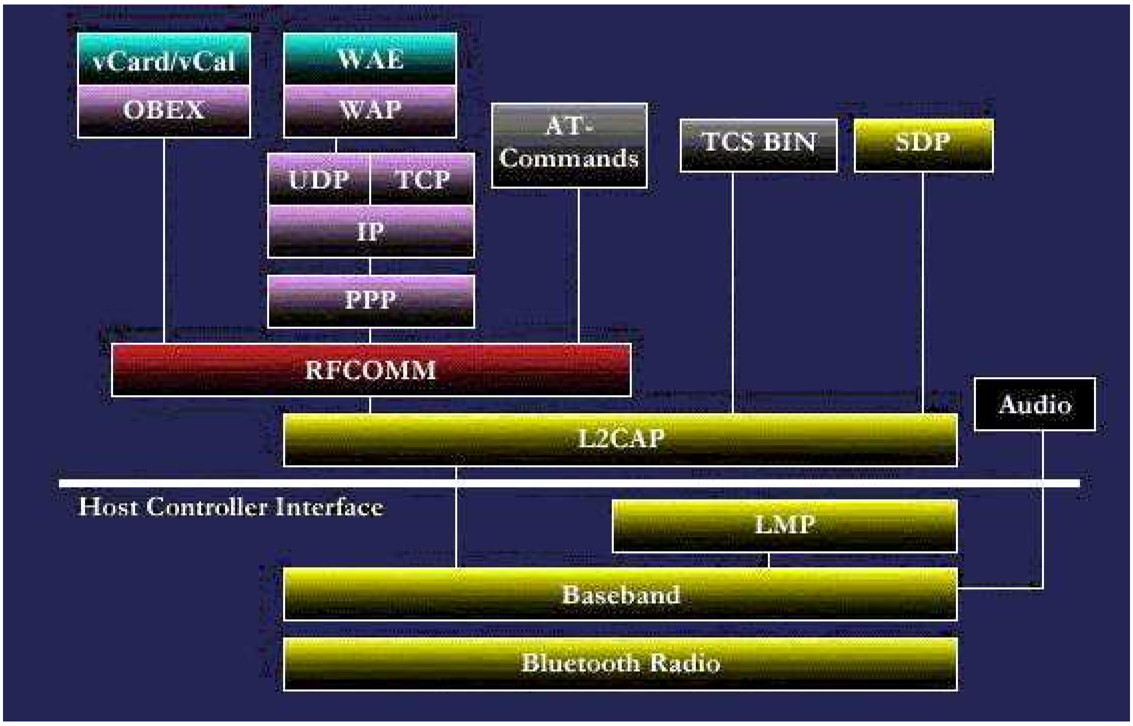

*Fig 1:The Bluetooth Protocol Stack Model*

The protocols and layers in the Bluetooth protocol stack

| **Protocol Layer** | **Protocols in the stack** |
|---|---|
| Bluetooth Core Protocols | Baseband, LMP, L2CAP, SDP |
| Cable Replacement Protocol | RFCOMM |
| Telephony Control Protocol | TCS Binary, AT-commands |
| Adopted Protocols | PPP, UDP/TCP/IP, OBEX, WAP, vCard, vCal, IrMC, WAE |

In addition to the above protocol layers, the Specification also defines a Host Controller Interface (HCI). This provides a command interface to the baseband controller, link manager, and access to hardware status and control registers.

The Bluetooth Core protocols (plus the Bluetooth radio) are required by most of Bluetooth devices while the rest of the protocols are used only as needed. The combination of the Cable Replacement layer, the Telephony Control layer and the adopted protocol layer form the application-oriented protocols which enable applications to run over the Bluetooth Core protocols.

The Bluetooth Protocol Architecture has been developed by the Bluetooth Special Interest Group (SIG) are intended for rapidly developing applications using Bluetooth technology. The lower layers of the Bluetooth stack are designed to provide a flexible base for further protocol development. RFCOMM protocols are adopted from existing protocols and these protocols and have been only slightly modified for the purpose of Bluetooth. The upper layer protocols are used without modifications this has been to allow existing applications to be reused to work with the Bluetooth technology and the interoperability is ensured more easily.

# Core Protocols

## Baseband

The Baseband and Link Control layer enables the physical RF link between Bluetooth forming a piconet. As the Bluetooth RF system is a

Frequency-Hopping-Spread-Spectrum system, in simpler terms packets are transmitted in defined time slots on defined frequencies. This synchronizes the transmission hopping frequency and clock of different Bluetooth devices.

It provides two different kind of physical links with their corresponding baseband packets, Synchronous Connection-Oriented and Asynchronous Connectionless which can be transmitted in a multiplexing manner on the same RF link.Asynchronous Connectionless (ACL) packets are used for the transmission of data only while Synchronous Connection-Oriented can contain audio only or a combination of audio and data.

All audio and data packets can be provided with different levels of FEC or CRC error correction and can be encrypted. Furthermore, the different data types, including link management and control messages, are each allocated a special channel

Audio data can be transferred between one or more Bluetooth devices, making various usage models possible and audio data in SCO packets is routed directly to and from Baseband and it does not go through L2CAP. Audio model is relatively simple within Bluetooth; any two Bluetooth devices can send and receive audio data between each other just by opening an audio link.

## Link Manager Protocol

The link manager protocol is responsible for link set-up between Bluetooth devices. This includes setting up of security functions like authentication and encryption by generating, exchanging and checking of link and encryption keys and the control and negotiation of baseband packet sizes. Furthermore it controls the power modes and duty cycles of the Bluetooth radio device, and the connection states of a Bluetooth unit in a piconet.

## Logical Link Control and Adaptation Protocol

The Bluetooth logical link control and adaptation protocol (L2CAP) adapts upper layer protocols over the baseband. It can be thought to work in parallel with LMP in difference that L2CAP provides services to the upper layer when the payload data is never sent at LMP messages.

L2CAP provides connection-oriented and connectionless data services to the upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length. Although the Baseband protocol provides the SCO and ACL link types,L2CAP is defined only for ACL links and no support for SCO links is specified in Bluetooth Specification 1.0.

## Service Discovery Protocol

Discovery services are crucial part of the Bluetooth framework. These services provide the basis for all the usage models. Using SDP, device information, services and the characteristics of the services can be queried and after that, a connection between two or more Bluetooth devices can be established. SDP is defined in the Service Discovery Protocol specification.

# Telephony and Cable Replacement Protocol

Telephony Control protocol - Binary (TCS Binary or TCS BIN), a bit oriented protocol, defines the call control signaling for the establishment of speech and data calls between Bluetooth devices.

In addition, it defines mobility management procedures for handling groups of Bluetooth TCS devices. TCS Binary is specified in the Bluetooth Telephony Control protocol Specification Binary, which is based on the ITU-T Recommendation Q.931, applying the symmetrical provisions as stated in Annex D of Q.931

## RFCOMM

RFCOMM is a serial line emulation protocol and is based on ETSI 07.10 ( European Telecommunications Standardization Institute ) specification. This ~Scable replacement~T protocol emulates RS-232 control and data signals over Bluetooth baseband, providing both transport capabilities for upper level services (e.g. OBEX) that use serial line as transport mechanism. RFCOMM is specified in.

# Adopted Protocols

## PPP

In Bluetooth technologies PPP is designed to run over RFCOMM to accomplish point to point connection.

PPP is the IETF Point-to-Point Protocol (Internet Engineering Task Force, IETF Directory List of RFCs) and PPP-Networking is the means of taking IP packets to/from the PPP layer and placing them onto the LAN.

## TCP/UDP/IP

These protocol standards are already defined by the Internet Engineering Task Force and used commonly in communication across the Internet (Internet Engineering Task Force, IETF Directory List of RFCs). The TCP/IP stacks are used in numerous devices including printers, handheld computers and mobile handsets the use of the TCP/IP protocol in the Bluetooth Specification Protocol for the implementation in Bluetooth devices allows for communication with any other device connected to the Internet. The Bluetooth device should be a Bluetooth cellular handset or a data access point for example is then used as a bridge to the Internet. TCP/IP/PPP is used for the all Internet Bridge usage scenarios in Bluetooth 1.0 and for OBEX in future versions. UDP/IP/PPP is also available as transport for WAP.

## OBEX Protocol

IrOBEX (shortly OBEX) is a session protocol developed by the Infrared Data Association (IrDA) to exchange objects in a simple and spontaneous manner. OBEX, which provides the same basic functionality as HTTP but in a much lighter fashion, uses a client-server model and is independent of the transport mechanism and transport API, provided it realizes a reliable transport base. Along with the protocol itself, the "grammar" for OBEX conversations between devices, OBEX also provides a model for representing objects and operations. In addition, the OBEX protocol defines a folder-listing object, which is used to browse the contents of folders on remote device. In the first phase, RFCOMM is used as sole transport layer for OBEX . Future implementations are likely to support also TCP/IP as a transport.

### Content Formats

vCard (The Internet Mail Consortium, vCard - The Electronic Business Card Exchange Format) and vCalendar (The Internet Mail Consortium, vCalendar - The Electronic Calendaring and Scheduling Exchange Format) are open specifications developed by the versit consortium and now controlled by the Internet Mail Consortium. These specifications define the format of an electronic business card and personal calendar entries and scheduling information, respectively. vCard and vCalendar do not define any transport mechanism but only the format under which data is transported. By adopting the vCard and vCalendar, the SIG will help further promote the exchange of personal information under these well defined and supported formats. The vCard and vCalendar specifications are available from the Internet Mail Consortium and are being further developed by the Internet Engineering Task Force (IETF).

Other content formats, which are transferred by OBEX in Bluetooth, are vMessage and vNote . These content formats are also open standards and are used to exchange messages and notes. They are defined in the IrMC (Infrared Mobile Communications) specification, which also defines a format for the log files that are needed when synchronizing data between devices.

## WAP

The main advantage of using WAP features in Bluetooth technologies is to build application gateways, which will mediate between WAP servers and some other application on the PC. In simpler terms, this will provide functions like remote control and data fetching from PC to handset. The idea behind the use of WAP is to reuse the upper software application developed for the WAP Application Environment Bluetooth Usage Models and Protocols.

# Usage Models

In the following text, the highest priority usage models identified by the SIG’s marketing group are briefly introduced. Each usage model is accompanied by a Profile.

Profiles define the protocols and protocol features supporting a particular usage model. Bluetooth SIG has specified the profiles for these usage models. In addition to these profiles, there are four general profiles that are widely utilized by these usage model oriented profiles. These are the generic access profile (GAP), the serial port profile, the service discovery application profile (SDAP), and the generic object exchange profile (GOEP).

## File Transfer

The file transfer usage model (See also the file transfer profile) offers the ability to transfer data objects from one device (e.g., PC, smart-phone, or PDA) to another. Object types include, but are not limited to, .xls, .ppt, .wav, .jpg, and .doc files, entire folders or directories or streaming media formats. Also, this usage model offers a possibility to browse the contents of the folders on a remote device.

In the following figure, the required protocol stack presented for this usage model is presented. The figure does not show the LMP, Baseband, and Radio layers although those are used underneath (See Figure 2).

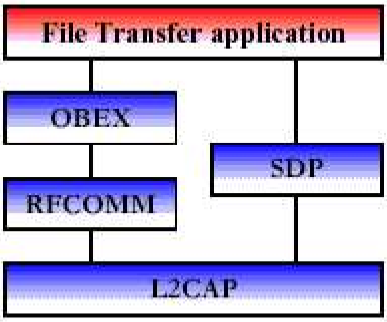

*Fig 1: Protocol Stack for File Transfer Applications*

# Synchronization

The synchronization usage model provides a device-to-device (phone, PDA, computer, etc.) synchronization of the PIM (personal information management) information, typically phonebook, calendar, message, and note information. Synchronization requires business card, calendar and task information to be transferred and processed by computers, cellular phones and PDAs utilizing a common protocol and format. The protocol stack for this usage model is presented in Figure 4. In the figure, the synchronization application block represents either an IrMC client or an IrMC server software.

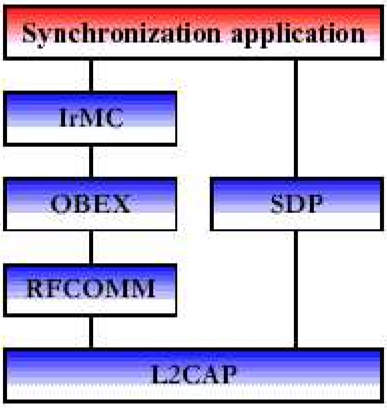

*Fig 2: Protocol Stack for Synchronization*

# Three-in-One Phone

Telephone handsets built to this profile may connect to three different service providers. First, telephones may act as cordless phones connecting to the public switched telephone network (PSTN) at home or the office and incurring a fixed line charge. This scenario includes making calls via a voice base station, making direct calls between two terminals via the base station and accessing supplementary services provided by an external network. Second, telephones can connect directly to other telephones for the purpose of acting as a ~Swalkie-talkie~T or handset extension. Referred to as the intercom scenario , the connection incurs no additional charge. Third, the telephone may act as a cellular phone connecting to the cellular infrastructure and incurring cellular charges. The cordless and intercom scenarios use the same protocol stack, which is shown in Figure 5. The audio stream is directly connected to the Baseband protocol indicated by the L2CAP bypassing audio arrow.

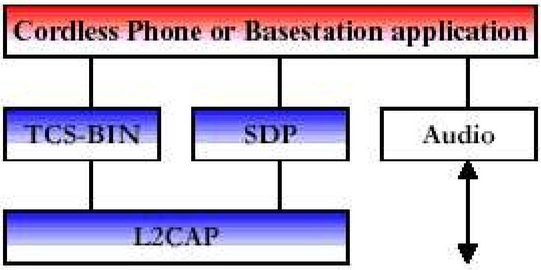

*Fig 3:Protocol Stack for Cordless Phone and Intercom Scenarios*

## Ultimate Headset

The headset can be wirelessly connected for the purpose of acting as a remote device~Rs audio input and output interface. The headset increases the user~Rs freedom of movement while maintaining call privacy. A common example is a scenario where a headset is used with either a cellular handset, cordless handset, or personal computer for audio input and output. The protocol stack for this usage model is depicted in Figure 6. The audio stream is directly connected to the Baseband protocol indicated by the L2CAP bypassing audio arrow. The headset must be able to send AT-commands (Attention commands) and receive result codes. This ability allows the headset to answer incoming calls and then terminate them without physically manipulating the telephone handset.

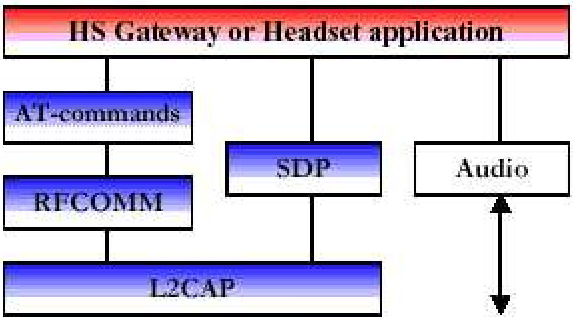

*Fig 4: Ultimate Headset Protocol Stack*

# Establishing Connections in Bluetooth

This section describes the basic procedures to be followed by two or more Bluetooth devices to start a connection between themselves (Bluetooth Connect Without Cables by Jennifer Bray and Charles F Sturman). Consider the following scenario: A person walks in to a hotel lobby and wants to access her email over her Bluetooth enabled device, which could be a laptop or a Personal Digital Assistant. What would she have to do?

Depending on the implementation., she would be clicking on a menu or an email application icon. The device would automatically carry out the following steps, (except perhaps for the authentication step if the device has come to the environment for the first time):

1. **Inquiry:** The device on reaching a new environment would automatically initiated an inquiry to find out what access points are within its range. (If not, it’ll do so when the email application asks for a link.) This will result in the following events:
   a. All nearby access points respond with their addresses.
   b. The device picks one out the responding devices.
2. **Paging:** The device will invoke a baseband procedure called paging. This results in synchronization of the device with the access point, in terms of its clock offset and phase in the frequency hop, among other required initializations.

3. **Link establishment:** The LMP will now establish a link with the access point. As the application in this case is email, an ACL link will be used. Various setup steps will be carried out as described below.
4. **Service Discovery:** The LMP will use the SDP (Service Discovery Protocol) to discover what services are available from the access point, in particular whether email access or access to the relevant host is possible from this access point or not. Let us assume that the service is available, otherwise, the application cannot proceed further. The information regarding the other services offered at the access point may be presented to the user.
5. **L2CAP channel:** With information obtained from SDP, the device will create an L2CAP channel to the access point. This may be directly used by the application or another protocol like RFCOMM may be run over it.
6. **RFCOMM channel:** Depending on the need of the email application an RFCOMM or other channel (in case of other applications) will be created over the L2CAP channel. This feature allows existing applications developed for serial ports to run without modification over Bluetooth platforms.
7. **Security:** If the access point restricts its access to a particular set of users or otherwise offers secure mode communications to people having some prior registration with it, then at this stage, the access point will send a security request for "pairing". This will be successful if the user knows the correct PIN code to access the service. Note that the PIN is not transmitted over the wireless channel but another key generated from it is used, so that the PIN is difficult to compromise. Encryption will be invoked if secure mode is used.
8. **PPP:** If a PPP link is used over serial modem as in dial up networking, the same application will now be able to run PPP over RFCOMM (which emulates the serial port). This link will allow the user to login to his email account.
9. **Network Protocols:** The network protocols like TCP/IP, IPX , Appletalk can now send and receive data over the link.

In the above procedure, user interaction is required only at the usual login for his email and additionally for the security to be implemented. The remaining steps are automatic.

# Bluetooth Security

Bluetooth has powerful security features with the SAFER+ (Secure And Fast Encryption Routine) encryption engine using up to 128 bit keys (Bluetooth Connect Without Cables by Jennifer Bray and Charles F Sturman).

At the Link Level, it is possible to authenticate a device. This verifies that a pair of devices share a secret key derived from a Bluetooth passkey, also known as a Personal Identification Number (PIN). The Bluetooth passkey is entered either in a user interface or for devices such as headsets, which do not have a user interface, the manufacturer can build it in.

After authentication, devices can create shared link keys, which can be used to encrypt traffic on a link. The combination of authentication and creating link keys is calling pairing, possibly accompanied by exchange of higher-level security information, and is called bonding.

Authentication may be repeated after pairing, in which case the link key is used as the shared secret key.

Three modes of security can be implemented: Mode 1 is not secure, Mode 2 has security imposed at the request of applications and services, and Mode 3 has security imposed when any new connection is established.

# Competing Technologies

Bluetooth is emerging as the preferred wireless technology for WPAN (Bluetooth Technology Overview, White Paper). The only other competing technology is Infrared Technology, known as IrDA.

IrDA is the most economical wireless connectivity solution to implement. In spite of an installed base of over 100 million units worldwide, a series of limitations greatly reduces its potential. Although operating at a transfer rate of 4 Mbps, greater than that of Bluetooth, IrDA requires line-of-sight between appliances which significant reduces usability, its short operating range of 1 meter is a major limitation that will allow Bluetooth to eventually replace it.

Given the fact that IrDA will enjoy a significant edge over Bluetooth in terms of installed base, IrDA will likely continue to be integrated into notebook computers and other handheld devices. As the installed base for Bluetooth grows the need for IrDA will likely decrease; however, this is not expected for several years. For the near to medium term IrDA and Bluetooth will likely coexist.