

1

Overview

Bluetooth has been the subject of much hype and media attention over the last couple of years. As various manufacturers prepare to launch products using Bluetooth technology, an unsuspecting public is about to be catapulted into the next stage of the information technology revolution.

Bluetooth is a low cost, low power short-range radio technology originally developed as a cable replacement to connect devices such as mobile phone handsets, headsets, and portable computers. This in itself sounds relatively innocuous; however, by enabling standardised wireless communications between any electrical devices, Bluetooth has created the notion of a Personal Area Network (PAN), a kind of close range wireless network that looks set to revolutionise the way people interact with the information technology landscape around them.

No longer do people need to connect, plug into, install, enable or configure anything to anything else. Through a ubiquitous standardised communications subsystem, devices will communicate seamlessly. One does not need to know where one's cellular phone is, or even if it is switched on. As soon as the Web browser appears on the mobile computer screen, a link is established with the phone, the Internet Service Provider is connected to, and the user is surfing the Web.

The Bluetooth specification is an open, global specification defining the complete system from the radio right up to the application level. The protocol stack is usually implemented partly in hardware and partly as software running on a microprocessor, with

different implementations partitioning the functionality between hardware and software in different ways.

1.1 BLUETOOTH'S ORIGINS

Version 1.0 of the Bluetooth specification came out in 1999, but Bluetooth started five years earlier, in 1994, when Ericsson Mobile Communications began a study to examine alternatives to the cables that linked their mobile phones with accessories. The study looked at using radio links. Radio isn't directional, and it doesn't need line of sight, so it has obvious advantages over the infra-red links previously used between handsets and devices. There were many requirements for the study, including handling both speech and data, so that it could connect phones to both headsets and computing devices.

Out of this study was born the specification for Bluetooth wireless technology. The specification is named after Harald Blatand, a tenth century Danish Viking king who united and controlled Denmark and Norway. The name was adopted as Bluetooth wireless technology is expected to unify the telecommunications and computing industries.

1.2 THE BLUETOOTH SIG

The Bluetooth Special Interest Group (SIG) is a group of companies working together to promote and define the Bluetooth specification. The Bluetooth SIG was founded in February 1998 by the following group of core promoters:

- Ericsson Mobile Communications AB.
- Intel Corp.
- IBM Corp.
- Toshiba Corp.
- Nokia Mobile Phones.

In May 1998, the core promoters publically announced the global SIG and invited other companies to join the SIG as Bluetooth adopters in return for a commitment to support the Bluetooth specification. The core promoters published version 1.0 of the Bluetooth specification in July 1999, on the Bluetooth Web site, <http://www.bluetooth.com>. In December 1999, the Bluetooth core promoters group enlarged with the addition of four more major companies:

- Microsoft.
- Lucent.
- 3Com.
- Motorola.

1.2.1 Joining the Bluetooth SIG

Any incorporated company willing to sign the Bluetooth SIG membership agreement can join the SIG as a Bluetooth adopter company. To join the SIG, companies simply fill in a form on the Bluetooth Web site, www.bluetooth.com. This form commits SIG members to contributing any key technologies which are needed to implement Bluetooth.

This commitment to share technology means that Bluetooth SIG member companies who put their products through Bluetooth qualification are granted a free license to build products using the Bluetooth wireless technology. The license is important because there are patents required to implement Bluetooth; companies that do not sign the Bluetooth adopter's agreement will not be entitled to use the technology. This offer proved so attractive that by April 2000, the SIG membership had grown to 1790 members.

In addition to getting a free license to patents needed to implement Bluetooth wireless technology, Bluetooth SIG members also have permission to use the Bluetooth brand. There are restrictions on the use of the brand, and these are set out in the Bluetooth brand book. The trademark may only be used on products which prove they are correctly following the Bluetooth specification by completing the Bluetooth qualification program (a testing process).

To get the Bluetooth figure mark and instructions on how to use it, companies sign the Bluetooth trademark agreement, also available on www.bluetooth.com. Questions on the Bluetooth trademark can be emailed to brand.manager@Bluetooth.com.

1.2.2 Bluetooth SIG Organisation

At the head of the Bluetooth SIG is the program management board. This board oversees the operations of a number of other groups as shown in Figure 1-1.

The main work of defining the specification is done by the technical working groups. Adopter companies can apply to become associate members of the SIG; they may then apply to join working groups and hence contribute directly to the forming of Bluetooth specifications.

Sitting on the technical working groups is quite time-consuming and so many companies with valid comments on the specification, do not have the resources to sit on the working groups. These companies can pass comments via email to the writers of the standard, and can also participate in an online discussion forum on the Bluetooth Web site.

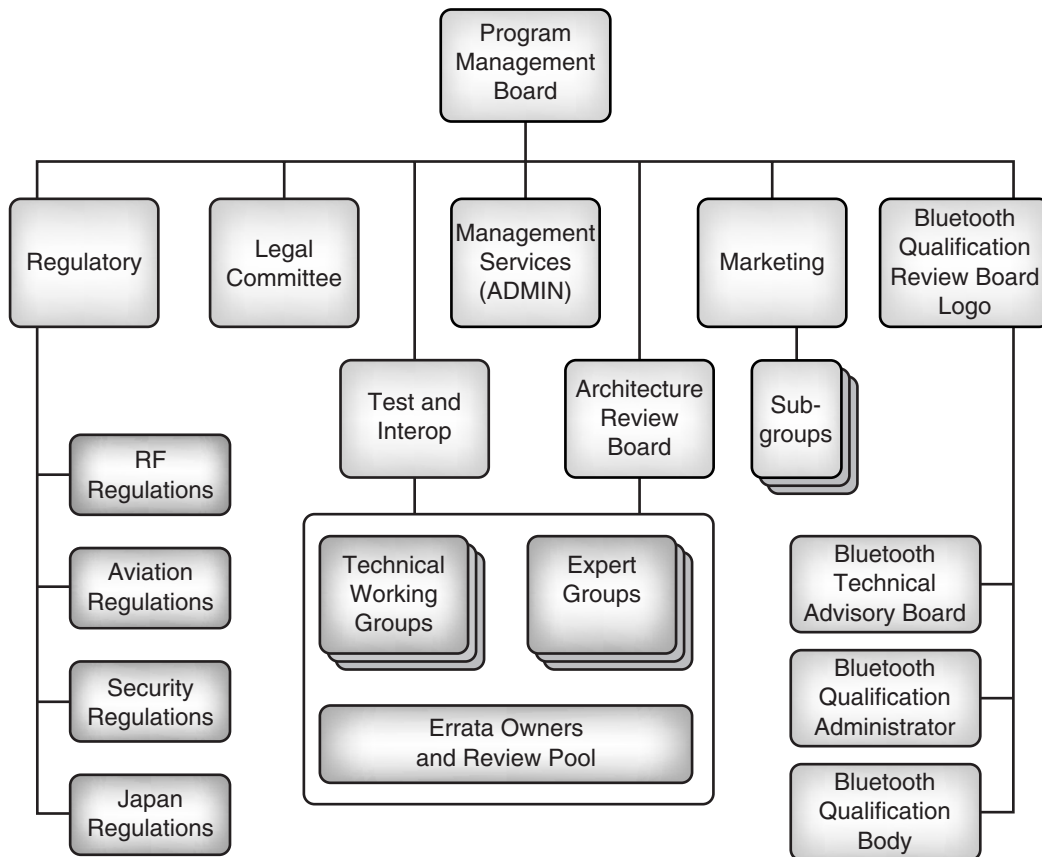


Figure 1-1 Organisation of the Bluetooth SIG.

1.3 AIMS

Why should a group with such diverse interests as the Bluetooth promoters cooperate? Basically because it's good for their businesses. The members of the Bluetooth promoters group all stand to gain something from mobile devices communicating better, whether by selling devices that have enhanced functionality, or by selling the extra software that people will need once they can more easily access information on the move.

The reasons for making the Bluetooth specification freely available to anyone who cares to sign an adopter's agreement are basically the same. The Bluetooth promoters group has made Bluetooth an open specification, rather than keeping it restricted and proprietary, because consumers are more likely to adopt a technology which can be bought from many manufacturers than one which is just limited to a select few. Wide acceptance

among consumers is likely to lead to a larger overall market for Bluetooth devices. So the promoters will gain from more companies becoming involved in the Bluetooth SIG.

The aim of the Bluetooth specification is basically to sell more of the core promoters' products. This will happen because Bluetooth will make their products more useful by improving communications between them. Before the advent of Bluetooth, telecommunications and computing devices were usually connected by cables, which were easily broken or lost. Cables are also awkward to carry around. The Bluetooth specification aimed to ease communication between mobile devices by providing a cable replacement.

Being a cable replacement technology imposes several requirements. If Bluetooth technology is to replace cables, it can't be much more expensive than a cable or nobody will buy it. At the time of writing, a data cable for a cellular mobile phone was about \$10. Allocate half the cost of the cable to each end of the link and it's obvious that for a cable replacement technology to be attractive on purely financial grounds, each unit should cost no more than \$5. So, the two ends of the link should cost the same as the cable they replace.

Because Bluetooth technology is designed for mobile devices, it must be able to run on batteries. So, it must be very low power, and should run on low voltages. It must also be lightweight and small enough not to intrude on the design of compact mobile devices such as cellular phones, headsets, and PDAs.

It must be as easy and convenient to use as plugging in a cable, and it must be as reliable as the cable it replaces. Because it is a wireless technology, to be reliable, Bluetooth must also be resilient. Reliability means it works overall; resilience means that it can cope with errors.

So, Bluetooth aims to be widely available, inexpensive, convenient, easy to use, reliable, small, and low power. If Bluetooth achieves all these goals, it will be incredibly good for the businesses involved with it.

1.4 THE PROTOCOL STACK

A key feature of the Bluetooth specification is that it aims to allow devices from lots of different manufacturers to work with one another. To this end, Bluetooth does not just define a radio system, it also defines a software stack to enable applications to find other Bluetooth devices in the area, discover what services they can offer, and use those services.

The Bluetooth stack is defined as a series of layers, though there are some features which cross several layers.

Every block in Figure 1-2 corresponds to a chapter in the core Bluetooth specification. The core specification also has three chapters on test and qualification:

- Bluetooth Test Mode.
- Bluetooth Compliance Requirements.
- Test Control Interface.

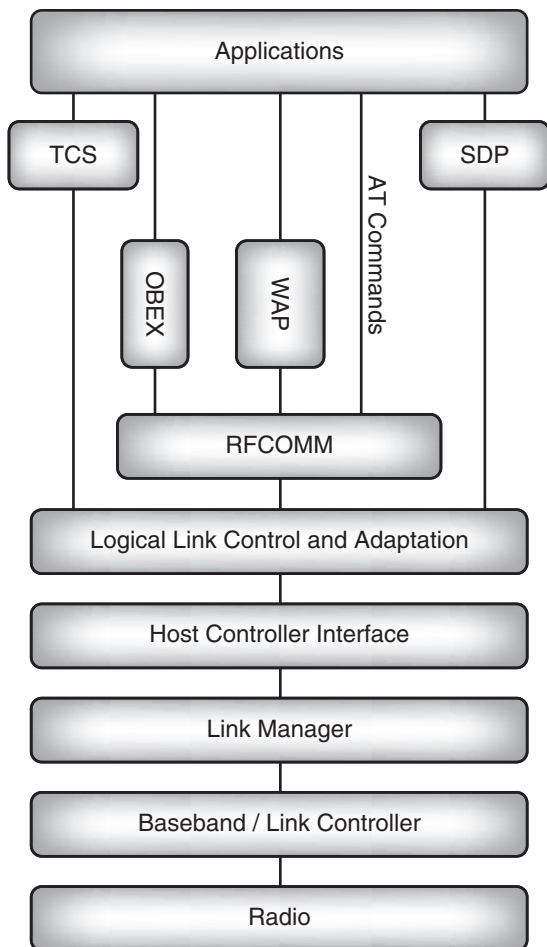


Figure 1–2 The Bluetooth protocol stack.

The Bluetooth specification encompasses more than just the core specification. There are also profiles which give details of how applications should use the Bluetooth protocol stack, and a brand book which explains how the Bluetooth brand should be used.

1.4.1 The OSI Reference Model

Figure 1–3 shows the familiar Open Systems Interconnect (OSI) standard reference model for communications protocol stacks. Although Bluetooth does not exactly match the model, it is a useful exercise to relate the different parts of the Bluetooth stack to the various parts of the model. Since the reference model is an ideal, well-partitioned stack, the comparison serves to highlight the division of responsibility in the Bluetooth stack.

The Physical Layer is responsible for the electrical interface to the communications media, including modulation and channel coding. It thus covers the radio and part of the baseband.

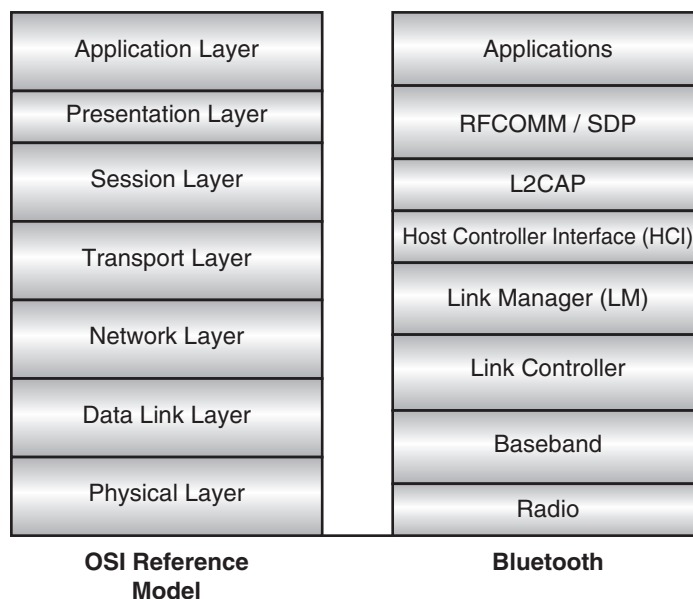


Figure 1-3 OSI reference model and Bluetooth.

The Data Link Layer is responsible for transmission, framing, and error control over a particular link, and as such, overlaps the link controller task and the control end of the baseband, including error checking and correction.

From now on, it gets a little less clear. The Network Layer is responsible for data transfer across the network, independent of the media and specific topology of the network. This encompasses the higher end of the link controller, setting up and maintaining multiple links, and also covers most of the Link Manager (LM) task. The Transport Layer is responsible for the reliability and multiplexing of data transfer across the network to the level provided by the application, and thus overlaps at the high end of the LM and covers the Host Controller Interface (HCI), which provides the actual data transport mechanisms.

The Session Layer provides the management and data flow control services, which are covered by L2CAP and the lower ends of RFCOMM/SDP. The Presentation Layer provides a common representation for Application Layer data by adding service structure to the units of data, which is the main task of RFCOMM / SDP. Finally, the Application Layer is responsible for managing communications between host applications.

1.4.2 The Physical Layer

Bluetooth devices operate at 2.4GHz in the globally available, licence-free ISM band. This band is reserved for general use by Industrial, Scientific, and Medical (ISM) applications, which obey a basic set of power and spectral emission and interference specifications. This means that Bluetooth has to be very robust, as there are a great many existing users and polluters of this shared spectrum.

The operating band is divided into 1MHz-spaced channels, each signalling data at 1 Megasymbol per second so as to obtain the maximum available channel bandwidth. With the chosen modulation scheme of GFSK (Gaussian Frequency Shift Keying), this equates to 1Mb/s. Using GFSK, a binary 1 gives rise to a positive frequency deviation from the nominal carrier frequency, while a binary 0 gives rise to a negative frequency deviation.

After each packet, both devices re-tune their radio to a different frequency, effectively hopping from radio channel to radio channel (FHSS—frequency hopping spread spectrum). In this way, Bluetooth devices use the whole of the available ISM band and if a transmission is compromised by interference on one channel, the retransmission will always be on a different (hopefully clear) channel. Each Bluetooth time slot lasts 625 microseconds, and generally devices hop once per packet, which will be every slot, every 3 slots, or every 5 slots.

Designed for low-powered portable applications, the radio power must be minimised. Three different power classes are defined which provide operation ranges of approximately 10m, 20m and 100m: the lowest power gives up to 10m range, the highest up to 100m.

1.4.3 Masters, Slaves, Slots, and Frequency Hopping

If devices are to hop to new frequencies after each packet, they must all agree on the sequence of frequencies they will use. Bluetooth devices can operate in two modes: as a Master or as a Slave. It is the Master that sets the frequency hopping sequence. Slaves synchronise to the Master in time and frequency by following the Master's hopping sequence.

Every Bluetooth device has a unique Bluetooth device address, and a Bluetooth clock. The baseband part of the Bluetooth specification describes an algorithm which can calculate a frequency hop sequence from a Bluetooth device address and a Bluetooth clock. When Slaves connect to a Master, they are told the Bluetooth device address and clock of the Master. They then use this to calculate the frequency hop sequence. Because all Slaves use the Master's clock and address, all are synchronised to the Master's frequency hop sequence.

In addition to controlling the frequency hop sequence, the Master controls when devices are allowed to transmit. The Master allows Slaves to transmit by allocating slots for voice traffic or data traffic. In data traffic slots, the Slaves are only allowed to transmit when replying to a transmission to them by the Master. In voice traffic slots, Slaves are required to transmit regularly in reserved slots whether or not they are replying to the Master.

The Master controls how the total available bandwidth is divided among the Slaves by deciding when and how often to communicate with each Slave. The number of time slots each device gets depends on its data transfer requirements. The system of dividing time slots among multiple devices is called Time Division Multiplexing (TDM).

1.4.4 Piconets and Scatternets

A collection of Slave devices operating together with one common Master is referred to as a piconet (see Figure 1–4). All devices on a piconet follow the frequency hopping sequence and timing of the Master.



Figure 1-4 Point to point and point to multipoint piconets.

In Figure 1-4, the piconet on the left with only one Slave illustrates a point to point connection. The piconet on the right with three Slaves talking to the Master illustrates a point to multipoint connection. The Slaves in a piconet only have links to the Master; there are no direct links between Slaves in a piconet.

The specification limits the number of Slaves in a piconet to seven, with each Slave only communicating with the shared Master. However, a larger coverage area or a greater number of network members may be realized by linking piconets into a scatternet, where some devices are members of more than one piconet (see Figure 1-5).

When a device is present in more than one piconet, it must time-share, spending a few slots on one piconet and a few slots on the other. On the left is a scatternet where one device is a Slave in one piconet and a Master in another. On the right is a scatternet where one device is a Slave in two piconets. It is not possible to have a device which is a Master of two different piconets since all Slaves in a piconet are synchronised to the Master's hop sequence. By definition, all devices with the same Master must be on the same piconet.

In addition to the various sources of interference mentioned already, a major source of interference for Bluetooth devices will clearly be other Bluetooth devices. Although devices sharing a piconet will be synchronised to avoid each other, other unsynchronised piconets in the area will randomly collide on the same frequency. If there is a collision on a particular channel, those packets will be lost and subsequently re-transmitted, or if

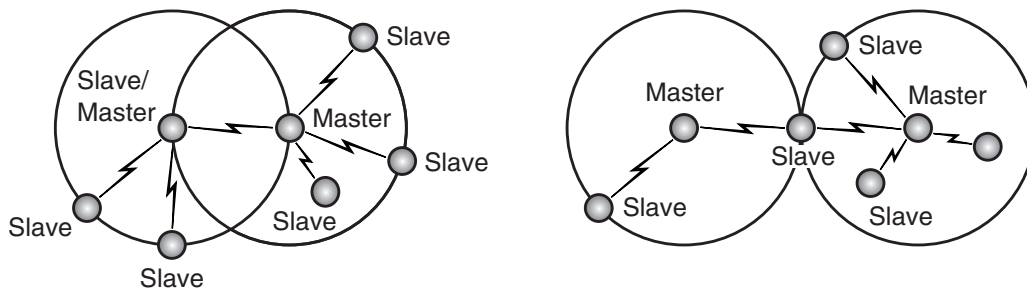


Figure 1-5 Scatternets.

voice, ignored. So, the more piconets in an area, the more re-transmissions will be needed, causing data rates to fall. This is like having a conversation in a noisy room: the more people who talk, the noisier it gets, and you have to start repeating yourself to get the point across.

This effect will happen if there are many independent piconets in one area, and it will also happen to scatternets, since the piconets making up the scatternet do not coordinate their frequency hopping.

1.4.5 Radio Power Classes

The Bluetooth specification allows for three different types of radio powers:

- Class 1 = 100mW (20 dBm).
- Class 2 = 2.5mW (4 dBm).
- Class 3 = 1mW (0 dBm).

These power classes allow Bluetooth devices to connect at different ranges. At the time of writing, most manufacturers are producing Class 1, low power, 1mW radios. These can communicate for a maximum of around 30 feet (10m). However, because things like bodies and furniture absorb microwaves, reception may not be reliable at the limit of this range. So, when using 1mW radios, a more realistic figure for reliable operation in a normal room will probably be 5m. This provides a low cost, low power communications solution which has plenty of range for a cable replacement technology.

Obviously, higher power radios have longer ranges. The maximum range for a Class 3, 100mW radio is about 100 metres. There is also a minimum range for a Bluetooth connection. If radios are put too close together, the receiver saturates; so, the minimum range for a Bluetooth radio link is around 10cm.

A 100m link needs a high power, Class 1 device at both ends, but it is possible to create piconets with a mixture of high and low power devices at different ranges. Figure 1–6 shows a mixture of high and low power devices in different piconets occupying an area.

This figure shows piconets which overlap with each other. This is possible because each Master has its own frequency hopping sequence, so two piconets are unlikely to be on the same frequency, at the same time. If they do meet on the same frequency, after the next frequency hop, they will not still be on the same frequency, so the data which may have been lost when the two piconets were on the same frequency can be resent.

1.4.6 Voice and Data Links

Bluetooth allows both time critical data communication such as that required for voice or audio, as well as high speed, time insensitive packet data communication. To carry such data, two different types of links are defined between any two devices. These are for voice communication: SCO (Synchronous Connection Oriented) links and for data communication: ACL (Asynchronous Connectionless) links.

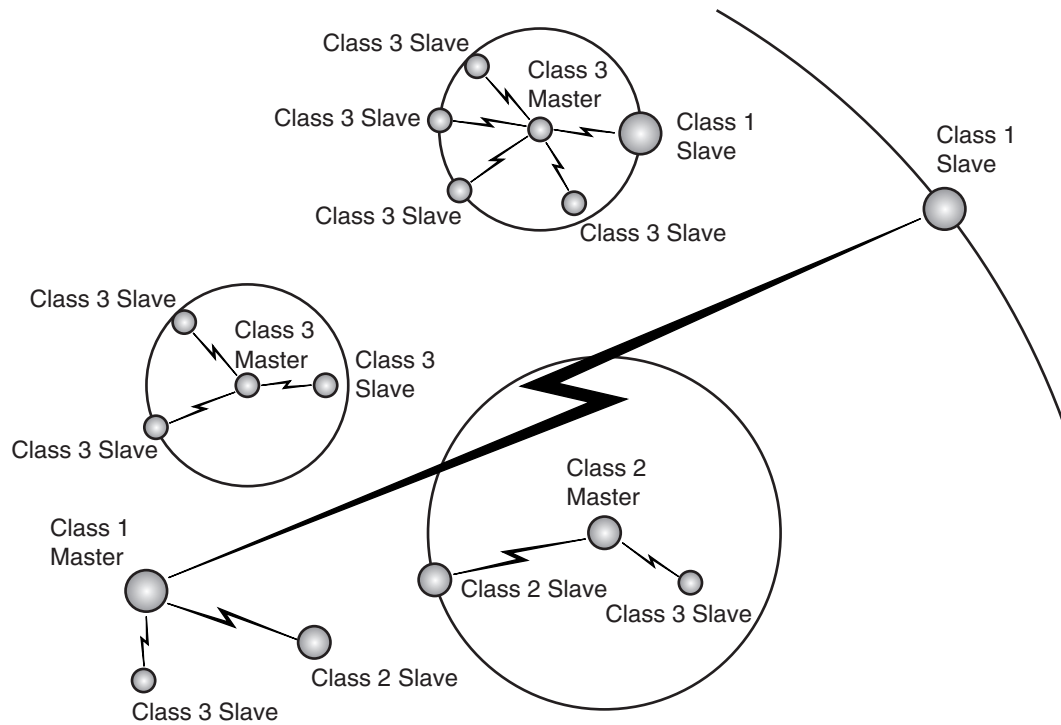


Figure 1-6 Piconets made up of different power class devices.

ACL data packets are constructed from a 72-bit access code: a 54-bit packet header and a 16-bit CRC code, in addition to the payload data. There are a variety of packet types allowing different amounts of data to be sent. The packet which carries the largest data payload is a DH5 packet, which stretches over five slots. A DH5 packet can carry 339 bytes, or 2712 bits of data. So, 2858 bits are sent on air for 2712 bits of information.

A DH5 packet uses up five slots, and the minimum length reply is one slot. Thus, the maximum baseband data rate in one direction is 723.2 Kb/s. In this case, with 5 slot packets sent in one direction, the 1 slot packets sent in the other direction will only carry 57.6 kb/s, so this would be an asymmetric link with more data going in the direction using 5-slot packets. If 5-slot packets were sent in both directions, the data rate obtained would be 43.9 kb/s, quite a reduction from the 1Mb/s data rate on air.

This overhead in both data encoding and frequency hopping is necessary mainly to provide a robust link since the ISM band is a shared resource with many devices, and indeed other communications standards and even noise sources cohabiting in the same spectrum. In addition, to further reduce the interference problem in the spectrum, national radio regulations limit the power emission per unit time in the ISM band, making a frequency hopping scheme necessary to spread transmissions over the spectrum and over time.

The higher layers of the protocol stack also use up some of the bandwidth, so at the application level, the maximum data rate could be around 650 kb/s.

The SCO links work at 64 kb/s, and it is possible to have up to three full-duplex voice links at once, or to mix voice and data. These voice channels give audio communication of a quality one would expect from a modern mobile cellular phone system such as GSM. As such, SCO links are not really suitable for delivering audio of a quality required for music listening.

One alternative to support music delivery is to use an ACL channel to carry audio. Raw CD-quality audio requires 1411.2 Kb/s, but with suitable compression, such as MP3 which reduces this bit rate to around 128 kb/s, near CD quality audio could easily be carried providing the time-criticality of the audio was maintained.

1.5 SECURITY

The high speed, pseudo-random frequency hopping algorithm employed in Bluetooth makes it very difficult to listen in on a Bluetooth connection. In fact, the U.S. military considers a communications link using frequency hopping over 79 channels to be secure in itself.

For link encryption and authentication, Bluetooth uses a strong contemporary cipher algorithm available in the public domain called SAFER+, which generates 128-bit cipher keys from a 128-bit plain text input.

1.6 APPLICATIONS AND PROFILES

Looking back to Section 1.3, the Bluetooth specification aimed to produce convenient, reliable, resilient, cost effective, low power, short range voice and data communications. It has achieved all these, but what sort of applications does this enable?

At its most basic, Bluetooth wireless technology replaces a cable and untethers devices. This makes it suitable for short range connections between a variety of mobile devices such as:

- Mobile cellular phone to Public Switched Telephone Network (PSTN) through an access point.
- Mobile cellular phone to a notebook PC.
- Mobile cellular phone to a headset.
- LAN access points for laptops or palmtops.
- Notebook, palmtop, or other Internet access device to the Internet via a PSTN access point or access module.
- Communication between laptops and palmtops.

In addition to the core specification, which defines the Bluetooth wireless communications protocol, the Bluetooth specification includes a profiles document. Each profile describes how a particular application can be implemented, including which parts of the

core Bluetooth protocol should be used to support the profile. Version 1.0 of the Bluetooth specification provides profiles for all of the connections listed above.

1.7 USING BLUETOOTH

Bluetooth is unlike any wired network, as there is no need to physically attach a cable to the devices you are communicating with; indeed, you may not know exactly what devices you are talking to and what their capabilities are. To cope with this, Bluetooth provides inquiry and paging mechanisms and a Service Discovery Protocol (SDP).

This section examines how these mechanisms are used to allow Bluetooth devices to link up and use each other's services.

1.7.1 Discovering Bluetooth Devices

Imagine two Bluetooth enabled devices, say a cell phone and a laptop computer. The cell phone is capable of acting as a modem using the dial up networking profile, and it periodically scans to see if anyone wants to use it.

The user of the laptop opens up an application which needs a Bluetooth dial up networking connection. To use this application, the laptop knows it needs to establish a Bluetooth link to a device supporting the dial up networking profile. The first stage in establishing such a connection is finding out what Bluetooth enabled devices are in the area, so the laptop performs an inquiry to look for devices in the neighbourhood.

To do this the laptop transmits a series of inquiry packets, and eventually the cell phone replies with a Frequency Hop Synchronisation (FHS) packet. The FHS packet contains all the information that the laptop needs to create a connection to the cell phone. It also contains the device class of the cell phone, which consists of major and minor parts. The major device class tells the laptop that it has found a phone; the minor part says that the type of phone is a cellular phone. This exchange of messages is illustrated in Figure 1-7.

In the same way, every Bluetooth-enabled device in the area which is scanning for inquiries will respond with an FHS packet, so the laptop accumulates a list of devices.

What happens next is up to the designer of the application. The laptop could present the user with a list of all the devices it has found and let the user choose what to do next; but if it did that at this stage, all it could do was tell the user about the types of devices it has found. Instead of telling the user about the devices it has found, the application could automatically go on to the next stage and find out which devices in the area support the dial-up networking profile.

1.7.2 Connecting to a Service Discovery Database

To find out whether a device supports a particular service, the application needs to connect to the device and use the service discovery protocol (SDP). Figure 1-8 illustrates how this is done. First the laptop pages the cellular phone, using the information it gathered during inquiry. If the phone is scanning for pages, it responds, and an ACL baseband connection can be set up to transfer data between the two devices.

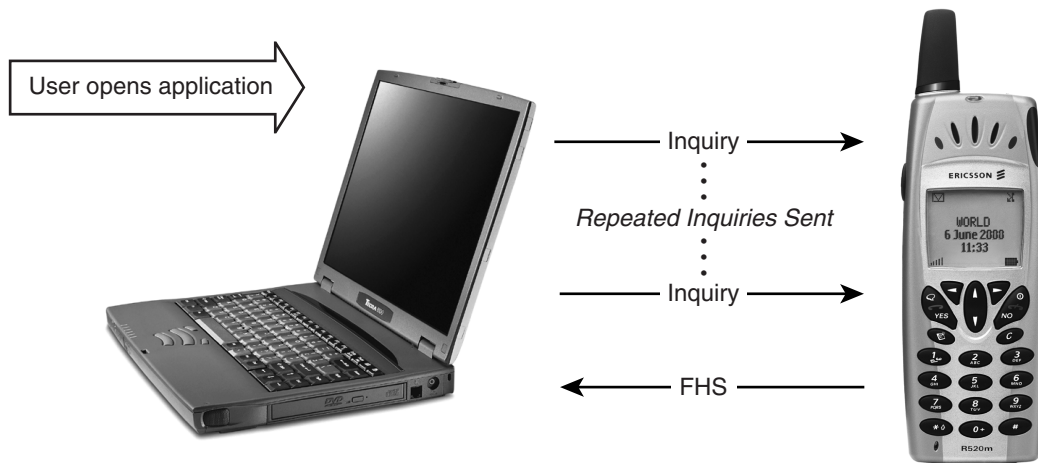


Figure 1-7 Discovering a Bluetooth device.

Once an ACL connection has been established, a Logical Link Control and Adaptation Protocol (L2CAP) connection can be set up across it. An L2CAP connection is used whenever data has to be transferred between Bluetooth devices. L2CAP allows many protocols and services to use one baseband ACL link. L2CAP distinguishes between different protocols and services using an ACL connection by adding a Protocol and Service Multiplexor (PSM) to every L2CAP packet. The PSM is different for every protocol or service that uses the link. Since this connection will be used for service discovery, its PSM = 0x0001, a special value that is always used for service discovery.

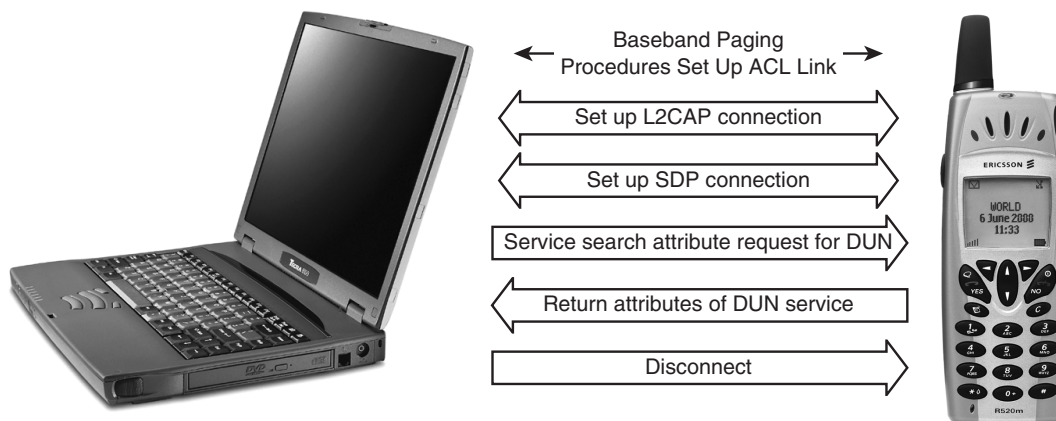


Figure 1-8 Retrieving information on services.

The laptop uses the L2CAP channel to set up a connection to the service discovery server on the cellular phone. The laptop's service discovery client can then ask the cellular phone's service discovery server to send it all the information it has relating to the dial up networking profile. The service discovery server on the cellular phone searches through its database and returns the attributes (characteristics) relating to dial up networking

Once the service discovery information has been retrieved, the laptop may decide to shut down the connection to the cellular phone. If the laptop wants to collect service discovery information from many devices in the area, then it makes sense to shut down the links after using them, since one device can only use a limited number of links at a time, and keeping the links alive will consume battery power unnecessarily.

After the laptop has collected service discovery information from devices in the area, what happens next is again up to the application. It could display the information on all devices it has found which support the dial up networking profile and let the user decide which one to connect to. Alternatively, the application could decide for itself which device to use without bothering the user.

Either way, the service discovery information tells the laptop everything it needs to know to connect to the dial up networking service on the cellular phone.

1.7.3 Connecting to a Bluetooth Service

The process of actually making a connection is shown in Figure 1-9. The paging process which establishes a baseband ACL link is the same as was used when connecting for service discovery.

This time the link is being set up for a protocol which may have particular quality of service requirements, so the application running on the laptop may wish to configure the link to meet its requirements. This is done by the application sending its requirements to

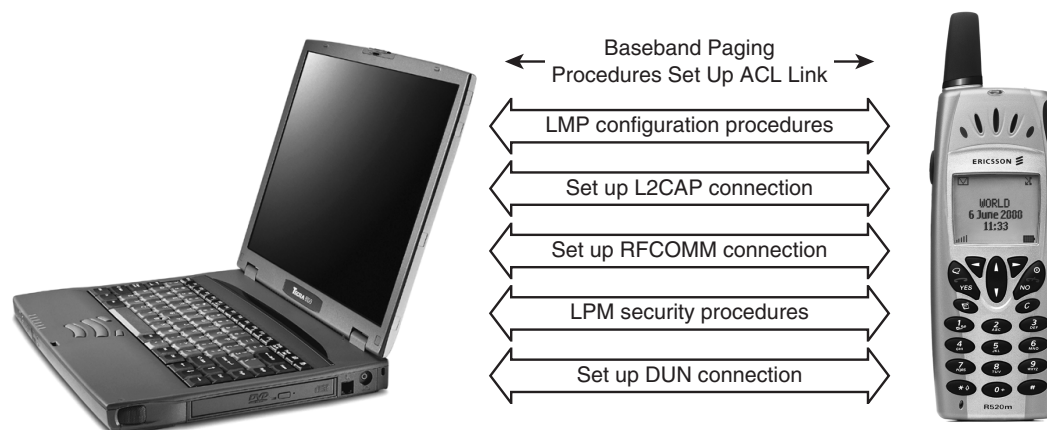


Figure 1-9 Connecting to a Dial Up Networking service.

the Bluetooth module using the Host Controller Interface. Next, the module's link manager configures the link using the link management protocol.

Once the ACL connection is set up to the laptop's satisfaction, an L2CAP connection is set up. The dial up networking profile uses RFCOMM, an RS-232 emulation layer, so the L2CAP connection uses the Protocol Stack Multiplexor for RFCOMM (PSM = 0x0003).

After the L2CAP link has been set up, an RFCOMM connection can be set up across it. RFCOMM, like L2CAP, can multiplex several protocols or services across one connection. Each protocol or service is given its own channel number. The cellular phone's channel number for Dial Up Networking was sent to the laptop in the service discovery information, so the laptop knows which channel number it should use when setting up the RFCOMM connection.

Finally, the Dial Up Networking (DUN) connection is set up using the RFCOMM connection, and the laptop can start to use the dial up networking services of the cellular phone.

Now, the laptop can use the cellular phone to make connections across the phone network without the two needing to be joined together by a data cable.

If the cellular phone is picked up and taken out of the range of the laptop, the laptop will have to repeat the procedure and find another device to connect to. Meanwhile, the cellular phone is still scanning and might be connected to another device elsewhere. The process of connecting is ad-hoc and arbitrary with Bluetooth connections, possibly only lasting for a short period of time as devices move around.

1.7.4 Discoverability and Connectability Modes

It is important to realise that for a connection to be established using Bluetooth wireless technology, both ends of the link have to be willing to connect.

Some devices may be set so that they will not scan for inquiries; in this case, other devices cannot discover them, and they will effectively be invisible. Similarly, some devices may be set so that they do not perform page scans. In these cases, they can still initiate connections, but they will not hear other devices trying to connect to them.

Applications can choose whether to make devices connectable or discoverable. A connection cannot be forced on a device which is not in the correct mode to accept it.

1.8 MANAGEMENT

Some parts of the Bluetooth system have to manage the links, establishing ACL links as needed and disconnecting when they are finished with them. L2CAP could fulfill this function, but since links must also be managed at the RFCOMM and SDP levels, it makes sense to have a separate device manager.

The core specification of Bluetooth does not say how the connections should be managed, although the security white paper gives some hints. The reason for this lack of mention in the specification is that device management does not affect end-to-end inter-operation, so it is safe to leave it up to individual implementers to find their own solutions. Furthermore, the most appropriate solution is likely to be different for different

devices. For instance, a headset only has to handle a single link, which is used for SDP and the headset service, so management is likely to be pretty simple, whereas a LAN access point has to juggle multiple links and balance bandwidth between them, so management of the links will be much more complex.

Bearing in mind that no single solution will be optimal for all possible devices, Figure 1–10 shows a possible protocol stack with a device and security manager that can handle establishment and configuration of the links.

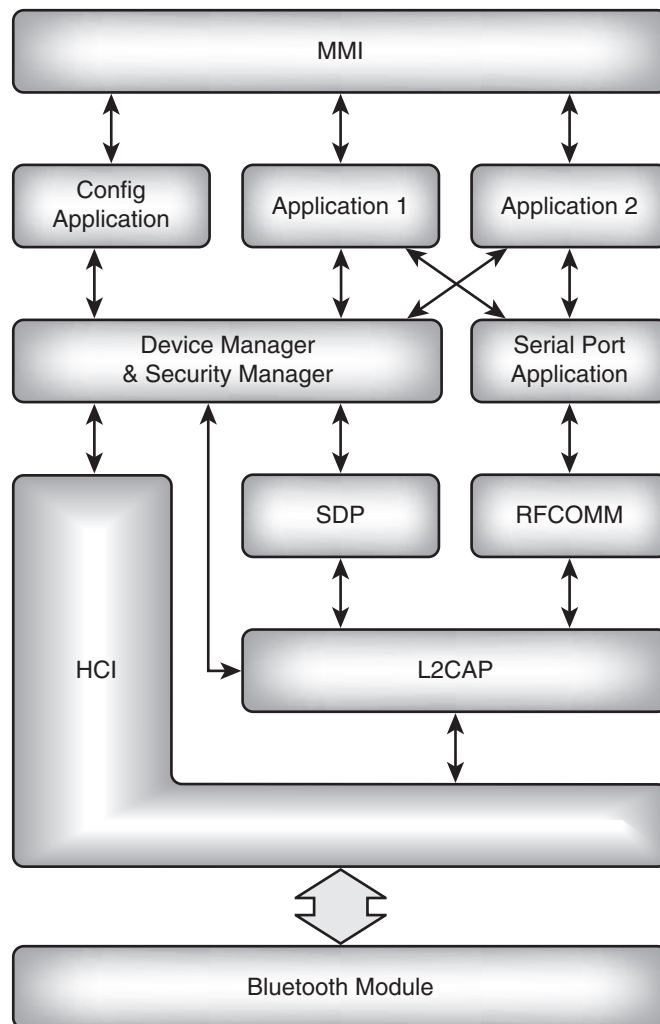


Figure 1–10 Management of the Bluetooth protocol stack.

The device manager interfaces to the HCI layer, SDP, RFCOMM, L2CAP, and to applications. It can provide the following facilities:

- Fault management—Detects, isolates, and corrects abnormal operation.
- Accounting management—Enables charging for use of managed objects and services.
- Configuration and name management—Controls, identifies, collects data from, and provides data to managed objects to assist in interconnection services.
- Performance management—Evaluates the behaviour of managed objects and the effectiveness of communication activities.
- Security management—Provides security management to protect managed objects and services.

Those familiar with the OSI model will recognise these facilities as those provided by OSI management.

Applications will have to register with the Bluetooth device manager to use Bluetooth links. They may then ask the device manager for connections, and request particular security and quality of service levels. If all applications go through the device manager, this allows it to create a database of higher layer protocols, applications, and services using links.

The device manager can also handle timeouts, shutting down links when they are no longer needed.

Bluetooth's management facilities do not have to be handled by a separate device management entity as described above. This function could be built into L2CAP, or into a profile application. However it is done, there must be some part of every Bluetooth implementation which handles management of the links.

1.9 TEST AND QUALIFICATION

The terms of the Bluetooth adopters agreement entitle all signatories to use the essential Intellectual Property Rights (IPR) underpinning Bluetooth free of charge. However, this entitlement for a particular product is conditional on that product passing successfully through the Bluetooth qualification program. To facilitate recognition in the marketplace of approved Bluetooth devices, qualification also entitles a product to use the Bluetooth brand. This mechanism makes it possible for the SIG to take legal proceedings against any non-conformant products which purport to offer Bluetooth functionality but fall short of the specification. The result is that the market should only see products which work reliably with all other Bluetooth products.

The requirements for qualification are split into four categories:

- Bluetooth radio link requirements.
- Bluetooth protocol requirements.
- Bluetooth profile requirements.
- Bluetooth information requirements.

In addition to the above, manufacturers must also ensure that the radio is tested appropriately to meet local radio emissions standards in the countries where it will be sold.

Interoperability tests must also be carried out to ensure that Bluetooth devices correctly implement the Bluetooth profiles, and can interwork with other devices implementing the same profiles. Devices can then be sold with a statement concerning which profiles they support so that it is perfectly clear to consumers which products they will work with and in what ways.

1.10 BLUETOOTH IN CONTEXT

Bluetooth does not exist in a vacuum. This section summarises some of the issues that affect Bluetooth devices which are not covered by the Bluetooth specification itself: how to implement Bluetooth, related technologies, the market for Bluetooth, health concerns, and the future of the specification.

1.10.1 Implementing the Technology

The key issue faced by implementers is that of partitioning. The hardware/software partition inside the Bluetooth subsystem trades off performance, cost, and power consumption against risk and time to market. The partition between the host system and the Bluetooth subsystem, is where (usually in software) the stack is partitioned. This will either add loading to the host's processing resources or require more performance and resources in the highly cost sensitive Bluetooth subsystem. Ultimately, the demand for a full implementation as a self contained, embedded Bluetooth solution will require very careful design and optimisation to avoid creating an un-commercial product.

The quality of the "user experience" is very important for any Bluetooth product and will also require careful design and a good understanding and specification of the target application. Bluetooth is going to be a very high volume system and demand very low cost with high levels of optimisation being crucial.

1.10.2 Related Technologies and Standards

Bluetooth, like most innovations throughout history, does not have the field to itself. There are many other initiatives and standards for wired and wireless data communications, either already deployed or under development. They vary between overlapping with Bluetooth's sphere of operation, while exhibiting clear differentiators to potential head-on competitors of Bluetooth. The two most active areas of work at the current time are the distribution of data and voice in a personal sphere of influence, the so called Personal Area Network (PAN) which appears to be Bluetooth's home ground, and the emerging demand for high speed wireless multimedia data distribution.

1.10.3 The Bluetooth Market

Most commentators agree that the Bluetooth market is going to be huge, with forecasts putting the installed base at half a billion devices by 2004, with a total market for Blue-

tooth components worth \$2 billion in the same year. It seems that for once, the technology push provided by Bluetooth is a good match for the market pull in terms of consumer needs and wants at this time.

There are a great many opportunities for Bluetooth-enabled products which exploit the various features of the technology to add value. However, there are many issues which are yet to be resolved. Potentially competing technologies could cause consumer confusion and at worst push Bluetooth into a niche corner. For manufacturers, the cost of the technology is paramount, and for Bluetooth to become ubiquitous, it must be built into all products, not just the high-end models.

For consumers, poor interoperability and/or poor user experience could be a major problem for Bluetooth and cause it to falter. The well-discussed "Out Of Box Experience" has to be seamless and simple. The hope is that the strength of the Bluetooth *brand* will promote the notion of reliability and ease-of-use.

1.10.4 Health

Bluetooth uses frequency spectrum in the range of 2400MHz to 2483.5MHz. This range encompasses the natural frequency of H₂O molecular oscillation at 2450MHz, which is also used by microwave ovens specifically to excite water molecules inside food in order to cook it.

Sharing the same frequency range as microwave ovens has led to some concerns that Bluetooth devices might *cook* their users. Some microwave radiation will be absorbed in flesh. It will be absorbed by field-induced rotation of polarized water molecules, which is converted to heat through molecular friction, basically, the microwaves shake the water in flesh, and it heats up as it shakes. But, as the radiated output power of Bluetooth devices is incredibly low and spread in spectrum in time, experts concur that Bluetooth radiation does not pose a risk to health.

A 1mW Bluetooth radio emits 1/1000,000, the amount of power in a 1KW microwave oven. Also, in a microwave oven, all the power is directed inward at the food, whereas in a Bluetooth device, the power is radiated outward, so the user only ever intercepts the smallest fraction of the radio waves which are heading in their direction.

It is interesting to compare bluetooth devices with other popular communications devices. Bluetooth operates at 2.4GHz and uses 1mW (0dBm) for most applications, with a maximum of 100mW (20dBm) for extended range. This means that Bluetooth signals have a penetration depth of only 1.5cm into flesh. In comparison, cellular handsets have a power of 10mW to 2W peak, using 450MHz to 2200MHz, and exhibit a penetration depth of 2.5cm in the middle of their range at 900MHz. So, mobile cellular handsets give rise to a measurable heating effect of 0.1°C, compared with no measurable increase for Bluetooth devices. Although studies have shown this small heating effect, it is too low to be noticed by the user. Most of the temperature increases that mobile phone users feel when holding a handset next to their ears is caused by an insulating effect. Since the head radiates a lot of heat, if a handset blocks that radiation, then the head heats up. Getting a hot ear from a mobile phone is not necessarily a sign that you are absorbing radiation!

There has already been some controversy regarding cellular handsets and whether they have a negative impact on health. Although scientific opinion is pretty conclusive

that there are no risks, to be safe, various organisations have undertaken studies and research and have laid down guidelines for exposure to radio frequencies.

The WHO, ICNIRP, and IEEE have developed Radio Frequency (RF) exposure recommendations and these guidelines have been adopted by many national authorities. In the usual way of health and safety guidelines, they incorporate large safety margins. The guidelines specify near-field¹ restrictions (referred to as SAR) between 10MHz, to 10GHz, which devices with an output power of less than 1.6mW are incapable of exceeding. So, all low-power Bluetooth devices will fall within these restrictions. Higher power Bluetooth devices may need to be tested for SAR limits, and this will be done as part of radio regulatory testing.

The guidelines also specify a standard for total RF exposure. This is given as a power density of 10W/m². This level of spectral density would require an unrealistic number of Bluetooth devices to operate continuously in a very small space, which would actually not be possible due to the limited spectrum in the ISM band.

Several expert panels formed from organisations such as WHO, ICNIRP, EC, and the Royal Society of Canada have debated the topic of health in the context of existing higher power cellular technology in recent years. They have all concluded that there is no credible or convincing evidence that RF exposure from wireless devices operating within accepted exposure limits causes adverse human health effects. They did, however, recommend additional research to clarify some areas and fill gaps in existing knowledge.

In conclusion, experts agree that Bluetooth devices are too low in power to have any negative health consequences, being as they are—even for the higher power devices—an order of magnitude lower in power than existing cellular devices which based on existing research and official guidelines have already been proven to be safe.

1.10.5 The Future

The Bluetooth SIG has a series of working groups continuing development of the Bluetooth specification in three key areas: correction and clarification of the version 1.0 specification, development of further profiles, and development of enhanced radio and baseband in version 2.0 of Bluetooth.

The SIG has also provided a mechanism for adopter companies to propose more profiles to facilitate optimized Bluetooth implementations for specific applications.

Version 2.0 of the specification is expected to provide a higher data rate for Bluetooth (between 2 and 10 Mb/s), to provide the multimedia distribution facilities which are becoming a key requirement for the future of information technology. Other work is underway to improve on the overall feature set of the 1.0 specification in areas such as link handover between devices in a way that is similar to that which occurs in mobile cellular phone networks.

¹Near field are those radio waves found close to an emitting device.

1.11 SUMMARY

The Bluetooth core promoters group has produced a specification for short-range, low-cost wireless communications. This is the Bluetooth core specification. The complete Bluetooth specification also includes profiles which detail how applications should use the Bluetooth protocol stack, and a brand book which covers how the Bluetooth brand should be presented.

The Bluetooth specification not only covers how to set up short-range wireless links, but also describes the Bluetooth qualification process. By putting their products through this process, companies that join the Bluetooth SIG can get a free license to use the Bluetooth wireless technology and Bluetooth brand.

Bluetooth wireless technology allows up to eight devices to connect together in a communicating group called a piconet. The maximum speed of a link in a piconet is 723.2 kb/s at the baseband layer (the data rate seen at the Application Layer will be lower due to the intervening layers of the protocol stack using some of the bandwidth). Different piconets can be linked into scatternets, but the data rate between scatternets will be lower than the rate possible within a single piconet.