Bluetooth

Bluetooth is a specification for short distance wireless communication between two devices.

Bluetooth Specifications

Fixed/Mobile	Mobile
Circuit/Packet	Both
Max Bandwidth	1Mb
Range	10 meters
Frequency	2.40GHz-2.483.5Ghz (U.S. and Europe) or 2.472Ghz-2.497Ghz (Japan)
Host Network	None
Definer	Bluetooth SIG

Bluetooth technology is named after Harald Bluetooth, a Danish king who managed to consolidate Denmark and a part of Norway in the 1900s. The choice for the name of this technology is a manifestation of how influential and central the companies from this region are to the telecommunications industry.

Bluetooth is a networking technology that does not rely on user control or large amounts of power. By keeping the transmission power to an extremely low setting (1 milliwatt), Bluetooth is ideal for mobile battery operated devices. Moreover, Bluetooth does not rely on the user since it can automatically detect and communicate with other Bluetooth deviceswithout any user input.

Bluetooth technology relies on two things, a radio frequency technology and the protocol software enabling it to transmit data to other devices. Bluetooth-capable devices can transmit data to other devices not within the line of sight of the user. It also enables different devices to communicate using certain rules such as the amount of data that will be sent, the type of communication between the devices

and the radio frequency or frequencies this communication will take place. These protocols ensure that Bluetooth devices experience the least amount of interference from other Bluetooth capable objects while communicating with each other.

Bluetooth RF Properties

Low energy radio waves are the principal transmission system in Bluetooth networking. The frequency of Bluetooth capable devices ranges from 2.402 GHz to as high as 2.480 GHz, a frequency range specifically reserved by international agreement for ISM or medical, industrial and scientific devices.

Transmission Capabilities

Other devices in the market that use the same ISM band are garage door openers, cordless phones, baby monitors, etc and all these devices contribute to the increase in the risk of interference among Bluetooth devices. To avoid this, Bluetooth devices only use about 1 miliwatt of power in transmitting its signals. This makes the effective range of a Bluetooth device about 32 feet or ten meters and thus limits the chances of interference from other nearby devices.

Nevertheless, the low transmission power requirement of Bluetooth devices make them capable of communicating with other Bluetooth devices not within their range of sight. This means that a Bluetooth device can still connect to a personal computer for file transfers even if the computer is in an entirely different room in the house.

Bluetooth is not a one-on-one data transmission technology so it can communicate with up to eight devices within its transmission radius at one time. A Bluetooth device will use at most 1600 different and randomly chosen frequencies every second within the course of its transmission to minimize the probability of other devices using the same frequency and to minimize interference time when it does coincide with another device using the same frequency.

Piconets or Personal Area Networks

A Bluetooth-capable device coming into range with another one will first determine if it has data to share or commands to transmit. This happens automatically and without any user input. Bluetooth-capable devices communicating with each other

within an area form a piconet or personal area network where devices integrate and synchronize their frequency-hopping to keep in touch with each other.

With the use of a specific evice addresses in Bluetooth capable devices, it is possible to create multiple piconets or personal area networks within the same area. This means that since a cordless phone base unit and handset communicate with each other using a specific address range range, they will not interfere with Bluetooth-capable devices in the same room. The Bluetooth network ignores any transmission from devices outside of its assigned address range. The addresses of these devices and the program that instructs these devices to listen and respond using a specific address range are programmed by the manufacturer to lessen interference and increase the efficiency in data transmission of Bluetooth devices.

Since each device in a piconet is synchronized in frequency-hopping, the risk of two piconets interfering with each other by being in the same frequency at the same time is very minimal. Moreover, since the piconets change frequencies 1600 times every second, a collision between two piconets will last only a fraction of a second. Corrective software in these Bluetooth devices will also correct any interference-consequent errors, thereby increasing the efficiency of network communication.

Bluetooth Power Classes

Bluetooth provides three types of power classes, although class 3 devices are not in general availability.

Type	Power Level	Operating Range
Class 3 Devices	100mW	Up to 100 meters
Class 2 Devices	10mW	Up to 10 meters
Class 1 Devices	1mW	0.1-10 meters

Bluetooth Security

Bluetooth security is based upon device authentication, not user authentication. Each device is either trusted or untrusted. Bluetooth devices are identified by unique 48-bit identifiers, much like Ethernet MAC addresses.

Bluetooth Security Modes

Bluetooth features three security modes.

Mode	Name	Description
1	Non-secure	No security is implemented
2	Service-level security	Access is granted to individual services
3	Link-level security	Security is enforced at a common level for all applications at the beginning of the connection

Bluetooth Security Levels

Bluetooth features three possible security levels.

Mode	Description
3	No authentication or authorization is required
2	Authentication is required; authorization is not required
1	Authorization and authentication are required

Bluetooth Security Weaknesses

Bluetooth weakness include:

- The Bluetooth challenge-response key generation is weak. This scheme may use a static number or a number for a period of time, which can reduce the effectiveness of the authentication.
- Bluetooth's challenge-response is simplistic. A one-way challenge for authentication is susceptible to man-in-the-middle attacks. Mutual authentication via user verification should be used.
- The keys used by Bluetooth are weak. The initialization key needs to be more robust and the unit key is a public-generated key that can be reused. A set of keys should be used instead.
- The master key is shared between Bluetooth connections. This key is a broadcast and should have a better scheme than what is used.

- The encryption algorithm scheme utilized in Bluetooth uses a single algorithm and allows repeat authentication. A more robust method that limits authentication and increases the encryption should be used.
- Bluetooth implementations normally imit the PIN number range. A PIN number is usually only four digits and the scalability for large environments is difficult.

Additional Sources of Information on Bluetooth Security

For more information on Bluetooth security, read Bluetooth Protocol and Security Architecture Review by Korak Dasgupta, or Overview of Ad Hoc and Bluetooth Networks.

Bluetooth versus Infrared

The major advantages of the Bluetooth technology over other communication technologies are its being cheap, wireless and automatic.
A data transmission technology comparable to Bluetooth is IrDA or infrared communication much like what your remote control devices use to control the TV, stereo, air conditioner etc. The big drawback of this type of technology, however, is the requirement that the two devices establishing a connection must be within sight of one another for transmission to take place. You can only control infrared devices by pointing the remote directly at the device or lining up the infrared ports of both IR capable devices.
Bluetooth devices can communicate with one another even when they are not in the same room. In fact, even in its low power setting, a Bluetooth device can communicate with another device that is within its ten-meter radius regardless of walls, windows, or other physical obstructions.

Infrared technology limits the device communications to one on one. Thus, an IR remote control can control only one electronic device at a time. On the other hand, Bluetooth devices are capable of communicating with multiple devices at any given time.
Infrared devices, however, are less susceptible to interference than Bluetooth devices. This means that you can be sure that the data will be sent to the intended recipient without any distortion or inaccuracies. Improvements in the Bluetooth technology however minimizes this problem by enabling the Bluetooth devices to

hop frequencies and communicate within a specific frequency range. Therefore, although there is still risk of interference, the chances of it happening are very minimal. If such occurs, it will happen only in a very brief period of time and a software will be available to correct any consequent distortion.

Source: http://www.tech-faq.com/bluetooth.html