Brisson Group, Inc.
34 Aqueduct Rd.
Wayland, MA 01778
508-653-4091, 508-653-4194 Fax
david@brissongroup.com

Bluetooth 1.1 Revives the Bluetooth Promise

by Troy Holtby
Bluetooth product manager, 3Com Corp., Santa Clara, Calif.

Imagine a world of wireless connections that let you exchange business cards and files of all kinds with co-workers. Picture using wireless technology to set up your own personal area network linking your PC to handheld devices, mobile phones, printers, scanners, fax machines, copiers, and more. Sounds impossible – not for long. The new Bluetooth 1.1 specification promises to make such affordable wireless connections an every day reality.

As delivered in its 1.0 version, however, Bluetooth failed to fully deliver on its promise due to unexpected interoperability issues. The crux of the problem? Bluetooth 1.0 defined specific functionality but did not mandate specific implementation criteria, leaving key parts of the specification open to interpretation.

As discussed in this paper, different implementations of the same function could introduce discrepancies significant enough to thwart the interoperability required for Bluetooth's widespread use and success. When a Bluetooth cell phone from vendor A does not work with a Bluetooth PC card from vendor B, the user is less than encouraged to buy the Bluetooth printer from vendor C. Fortunately, Bluetooth 1.1 addresses these interoperability issues to restore the technology's original promise.

The most significant change to Bluetooth in 1.1 involves authentication. Bluetooth communications are encrypted for security. When two Bluetooth devices try to establish a link, one of the first things they need to do is exchange keys confirming their identities. If the keys don't match, the two devices won't talk to each other.

Under Bluetooth 1.0, the two devices could get into an irreconcilable race condition during the initial link negotiation. The devices would execute the algorithm to generate the key, but each device would generate a different key. The problem revolves around timing. Generating the correct key depends on which device initiates the conversation (the master) and how fast the responding device (the slave) replies to the master's communications. If the slave can process information faster than the master, the ensuing race condition can leave each device calculating that it is the master. Based on that error, the devices failed to generate matching keys.

Bluetooth 1.1 rectifies this problem by more thoroughly defining the steps required for device authentication. Specifically, version 1.1 requires that each device confirms its role

in the master/slave relationship by reconciling and/or acknowledging which device initiated interaction.

A more basic interoperability issue concerns the harmonization of frequencies. Bluetooth divides the 2.4GHz frequency into 79 hops. Using a technique called frequency hopping spread spectrum to transmit data, the master and slave must synchronize their movements up and down the 2.4GHz frequency to maintain their connection. If they don't arrive at the same hop at the same time, the devices can't communicate.

Unfortunately, France, Japan and Spain and a few other countries use the 2.4GHz frequency for non-commercial purposes, such as military communications. To accommodate these countries, Bluetooth 1.0 defined a second hop count that avoided select areas of the 2.4GHz spectrum and divided the frequency into 23 hops. Devices built to work at 79 hops are incompatible with those built to work at 23 hops.

To address this problem, the Bluetooth Special Interest Group negotiated with the 23-hop countries to allow use of 79-hop equipment, which enabled Bluetooth 1.1 to eliminate the 23-hop option. All Bluetooth 1.1 devices use 79 hops to communicate within the 2.4GHz frequency.

Incompatible data formatting could also prevent interoperability in Bluetooth 1.0 devices. Bluetooth supports up to five slots per packet to reach its maximum data transfer rate of 720 Kbps per channel; however, not all Bluetooth devices support five-slot packets. If a master tries to send more slots-per-packet than the slave can support, communications fail.

Under Bluetooth 1.0, slave devices were unable to tell master devices how many slots could be used during communications. Bluetooth 1.1 fixes this problem by letting the slave communicate back to the master with information about how packet sizes. In version 1.1, a slave can tell a master to send fewer (or more) slots per packet when necessary.

On the surface, the issues above look trivial. But not to users experiencing incompatibility problems. Today, Bluetooth delivers on its promise. The Bluetooth 1.1 specification was finalized earlier this year, and vendors have begun shipping 1.1-compliant products. As users have more exposure to the latest generation of Bluetooth products and watch them work successfully in multi-vendor environments, Bluetooth's wireless dream will be realized and its promise fulfilled.

# # #