

Logitech for Business Whitepaper



Logitech Advanced 2.4 GHz Technology With Unifying Technology

Revision 070709

December 8, 2009

TABLE OF CONTENTS

1	INTRODUCTION: THE MOVE TO WIRELESS PERIPHERALS IN BUSINESS	3
2	SYSTEM OVERVIEW	4
2.1	NETWORK TOPOLOGY	4
2.2	MAIN FEATURES	4
2.3	UNIFYING NETWORK	5
3	ASSOCIATION MODEL	6
4	ENCRYPTION	7
4.1	ENCRYPTION ALGORITHM	7
4.2	GENERATION OF ENCRYPTION KEYS	8
5	FEATURES & PERFORMANCE	9
5.1	POWER CONSUMPTION	10

1 Introduction: The Move to Wireless Peripherals in Business

In today's workplace, businesses demand that employees be increasingly mobile to move quickly, with computer equipment in hand, between in-house meetings, office to home, office to offsite meetings, and to travel to distant locations. More and more companies are therefore prioritizing the adoption of both wireless networks and notebook computers to not only meet these mobility needs, but also to promote comfort and productivity for their busy employees.

This modern business place in turn demands mice and keyboards that complete the story of mobility, along with employee comfort and productivity that also have the highest-level of encryption and powerful connections even in the busiest of environments. And, businesses demand ease of integration that requires little to zero setup time.

Logitech offers a variety of wireless mice, keyboards, and mice + keyboard combinations which come standard with Logitech Advanced 2.4 GHz technology. This technology includes:

- 128-bit (AES) encryption between device and receiver
- Up to 3-years of battery life
- Range of up to 10 meters or 33 feet

With Logitech Advanced 2.4 GHz, your employees can get all the benefits of a cord with the convenience of wireless. And, Logitech's wireless mice and keyboards are easy to use – no software installation or pairing is required.

With the addition of products containing Logitech Unifying wireless technology, business customers can increase the convenience and productivity with a tiny, leave-in receiver which can be connected to multiple devices. Connect the compatible mice and keyboards you leave at home and the office without replugging or setting up, or take the notebook PC to a meeting and return to the office desk and start typing away on the keyboard without reconnecting or repairing.

The goal of this document is to highlight the main features of the Logitech Advanced 2.4 GHz proprietary wireless technology. The scope is limited to a high-level presentation of the Advanced 2.4 GHz technology.

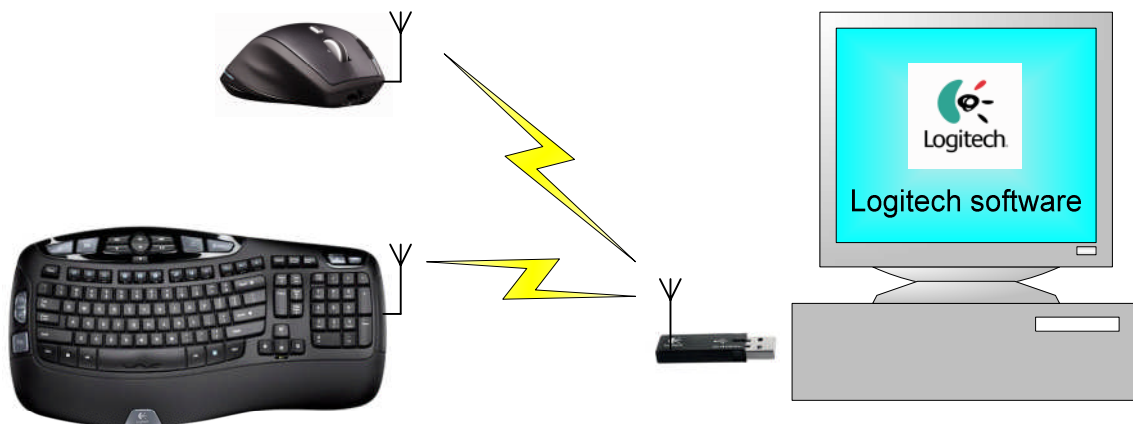
For a complete list of wireless mice and keyboards that contain Logitech Advanced 2.4 GHz wireless technology, please visit the Logitech for Business Products section at www.logitech.com/business. For more information on Unifying, visit www.logitech.com/unifying.

2 System Overview

2.1 Network Topology

An Advanced 2.4 GHz network is a star topology network where the receiver is the central point. Advanced 2.4 GHz typically supports one encrypted keyboard and one mouse connected to the same receiver. The Logitech software (SetPoint for PC or LCC for Mac) provides extra functionalities but is **not** mandatory to operate an Advanced 2.4 GHz network.

Unlike most star topology networks, the Advanced 2.4 GHz receiver is not the master of the links. Each device is a master and may transmit data at any time. This scheme contributes to further reduce the power consumption of the devices by shutting down their radio when no user activity is detected. The more common scheme where the receiver is continuously polling each device for data requires that the devices are continuously listening for the master.



2.2 Main Features

Unlike Bluetooth, Logitech Advanced 2.4 GHz is not a frequency-hopping protocol that continuously jumps from one channel to another. Logitech Advanced 2.4 GHz is a so-called frequency-agility protocol that stays on the same channel as long as possible. When the active channel becomes unusable, Logitech Advanced 2.4 GHz automatically selects another one.

The Advanced 2.4 GHz system uses 24 radio channels defined in the 2.4 GHz ISM band. This ISM band has the advantage of being available in most countries around the world.

The Advanced 2.4 GHz system implements only bidirectional links. Bidirectional links allow improved error correction, seamless encryption, device firmware upgrade and a better interaction between the Logitech software and the devices. The typical latency of an Advanced 2.4 GHz device operating in a clean environment is below 10 ms. In a noisy environment, this latency may increase depending on the strength, type and occurrence of the interference.

Communication between wireless keyboards and the receiver are always encrypted to avoid eavesdropping.

The Advanced 2.4 GHz devices are pre-paired to their receiver at the factory to be functional out-of-the box. The encryption keys required by the keyboard links are also pre-programmed at the factory.

An Advanced 2.4 GHz device can be replaced by another one at any time. The pairing procedure requires the Logitech Connect Utility software, and the communication will be automatically encrypted.

2.3 Logitech® Unifying Wireless Technology

Devices and receivers identified by the Unifying logo support the connection of up to 6 devices to the same receiver.

Unifying was developed to support the use case of mobile users who have one single receiver always plugged into their notebook, one set of keyboard and mouse in the office, another set at home, and a set of mobile devices when on the go.



Any combination of keyboards, mice, and number pads is allowed, as long as the total number of devices per receiver does not exceed 6, and as long as all devices and the receiver carry the Unifying logo.

3 Association Model

The association model defines the concepts and methods implemented to achieve a mutual recognition of wireless devices and their receivers.

To simplify the out-of-the-box product setup by the end user, the devices are pre-paired to their receiver at the factory. The factory pairing includes the generations of the encryption keys required by the keyboard links.

An optional Connect Utility software is available to pair or re-pair Advanced 2.4GHz devices to the original receiver.

If all devices and the receiver have the Unifying logo printed on them, the Logitech® Unifying software can be used to connect any configuration of up to 6 Unifying compatible devices (keyboards, mice or number pads) to a single Unifying receiver.

A command-line version of the Unifying software (called Logitech® Unifying Multi-Connect Utility) is available to help IT organizations to quickly assemble large quantities of custom Unifying configurations.

When the Logitech software detects that a second receiver was plugged, a wizard pops up to guide the user through the process of moving all Unifying compatible devices to the first receiver. When this is done, the second receiver can be removed to free up a USB port of the machine.

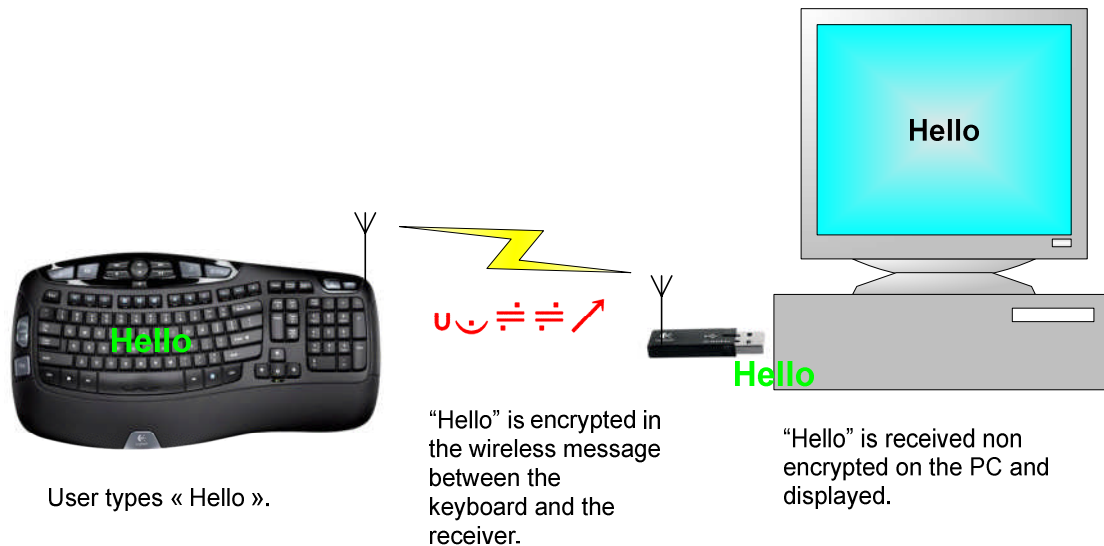
4 Encryption

Computer keyboards process very private or sensitive information like passwords, credit card numbers, or personal messages. Since the range of an Advanced 2.4 GHz device may reach several tens of meters in an open environment, it is critical to take adequate measures to prevent eavesdropping.

Advanced 2.4 GHz applies state-of-the-art encryption to the keyboard reports. Since the displacements of a mouse would not give any useful information to a hacker, the mouse reports are not encrypted.

Encryption is limited to the wireless link between keyboards and the receiver. Encryption is totally transparent to the software which receives clear data from the receiver over the USB. This means that the Advanced 2.4 GHz encryption provides no protection against hackers who are able to get physical access to the PC, or who are able to remotely install spy software on the PC.

The encryption applies to all standard keyboard keys (a, s, d, f...) and modifiers (Shift, Ctrl, Alt...). The multimedia keys (Play, Pause, Mute...) that may be implemented in some keyboards are transmitted in clear text.



4.1 Encryption Algorithm

The encryption method consists of hiding the wireless messages with a cryptogram. The selected algorithm is the AES 128-bit cipher, which has been adopted as an encryption standard by the US government. As of today, the only known way to crack it is to try all possible keys. Even if it was possible to test 1 billion keys per second, billions of years would be necessary to try all combinations.

AES is based on symmetric 128-bit keys, “symmetric” meaning that the same key is used to encrypt a message in the keyboard and to decrypt the message in the receiver

4.2 Generation of Encryption Keys

When a device that requires encryption is paired to a receiver, the pairing process includes the generation of 128-bit encryption keys. The same unique key is constructed both in the keyboard and in the receiver based on random values exchanged during the pairing procedure.

Note that the encryption keys are never transmitted over the air. By spying the packets exchanged during the pairing process, a hacker would not be able to find the encryption keys without knowing the secret algorithm implemented to construct them.

The initial encryption keys are programmed at the factory when the devices are paired to their receiver.

The encryption keys are stored in a non-volatile memory area of the keyboard and receiver. As this is hardware encrypted, software cannot access the keys.

5 Features & Performance

Transmission Parameters	
Radio frequency band	2.4 GHz ISM
Number of radio channels	24
Transmit power	0 dBm (like BT class 2 and Cypress WUSB)
Range: USB Micro receiver	10 m
Responsiveness	
Bandwidth (peak, raw)	2 Mbps bursts
Mouse report rate [rpts/s]	125 rpts/s
Keyboard typing speed [keys/s]	25 keys/s
Latency in a clean environment [ms]	< 8 ms
Latency following a power up [ms]	< 90 ms
Latency following low power mode [ms]	Implementation specific
Resistance to Interference	
Resistance to Wi-Fi perturbation	Good
Resistance to Bluetooth perturbation	Excellent
Resistance to Audio RF streamer (Logitech Z-5450)	Excellent
Resistance to Multipath effect (self-perturbation)	Excellent
Resistance to RF analog surveillance camera	Excellent
Exposition to interference in continuous tracking (= typical percentage of time during which the radio channel is used, and prone to collide with other radio traffic)	1-2%
Architecture Capabilities	
Keyboard encryption	Yes
Encryption method	AES 128 Bit
Downstream capability	Yes
Downstream bandwidth [kbits/s]	up to 20 kbits/s

Number of devices per dongle	up to 6 in Unifying networks, otherwise 2
Full SetPoint and LCC compatibility (proprietary extensions, HID++, Hi-Res roller etc...)	Yes

5.1 Power Consumption

In terms of power consumption, the main advantage of Advanced 2.4 GHz compared to a 27 MHz system is the available bit rate: 2 Mbits/s for Advanced 2.4 GHz vs. 6 kbits/s for 27 MHz. As a consequence, the time needed by an Advanced 2.4 GHz device to transmit a report is about 300 times shorter than the time needed by a 27 MHz device to transmit the same report. The radio of an Advanced 2.4 GHz device is therefore active for a much shorter period of time, leading to a lower average power consumption.



©2009 Logitech, Inc. All rights reserved. Logitech, the Logitech logo, and other Logitech marks are owned by Logitech and may be registered. All other trademarks are the property of their respective owners.