Methods of Synchronizing with a Bluetooth Piconet using CATC Bluetooth Analyzers – Merlin™, Merlin Mobile™, BT Tracer™ and Merlin II™

Application Note

Introduction

This application note examines various techniques for synchronizing a Bluetooth Analyser like the CATC Merlin to a Bluetooth Piconet and shows how and when you might use the different approaches.

In this paper we will use the terminology, ‘Bluetooth Master’ for the device, which initiates a Bluetooth connection and/or maintains a Piconet with one or more Bluetooth devices. A ‘Bluetooth Slave’ or ‘Target’ device is one that responds to the initiating device and/or is a subordinate unit of the piconet after it has been established.
Page sync and record

Requirements:
Slave BD_addr, Slave must support inquiry

Description:
CATC analyzer will inquire of the slave to recover the slave clock. The clock is used to listen to the same frequencies as the slave waiting for the master to page the slave. When the master pages the slave, the master clock is recovered and the hopping sequence of the piconet is determined.

When to Use:
Point-to-point Piconets where the slave is discoverable. This is preferred because it also verifies both the master and slave BD_address is correct/matches the selected values. Also to be used for multi-device piconets where recording is to start on the connection of a specific slave.

Tricks:
Use the “ANY” option in the master BD address when the master BD_address is not known. Don’t use this option in busy environments (e.g., unplugged fests) where many devices may inquire of the slave or where many piconets other than the desired ones are recorded.

Sync and record

Requirements:
Master BD_addr, master must support inquiry scan.

Description:
CATC analyzer will inquire of the master to get the master BT Clock. This allows the analyzer to follow the masters hopping sequence and follow any page to the master issues.

When to Use:
Multi-device piconets where master is discoverable, point-to-point piconets where the master is discoverable. This is preferred for piconets where the master will connect with more than one device.
Passive Sync and record

Requirements:
Master BD_addr, Slave BD_addr

Description:
In this mode the hopping sequence of the master and slave is not known. The CATC analyzer acts like a Bluetooth device with the Slaves BD_addr. When the master pages the slave, we hope the analyzer picks this up first and responds to the master with the cloned slave BD_Addr ID. The master then sends the FHS to the slave (analyzer) so the clock is recovered for the master. The analyzer then disappears and waits for the master to attempt paging the slave again.

When to Use:
When neither master or slave support inquiry is not discoverable, and the BD_address of both devices is known.

Cautions:
1) Real slave may respond before the analyzer to the master’s page. Allow 3-4 seconds for the initial page attempt before enabling the slave connection.
2) May fail if Masters BT Clock changes significantly after contacting analyzer and before contacting the slave (e.g master clock has significant drift or if master is powered off and on again after the first page attempt).

Tricks:
Set the slave address to some dummy value (e.g., 000000001) when you wish to start recording have the master attempt to page this dummy address. The analyzer will recover the masters BT clock and join the piconet. Note: if the link is to be encrypted, it is important that the analyzer joins the link prior to the start of the encryption.
This method can also be used to join established piconets where the master does not support inquiry during the piconet
Radio BT Tracer additional Options

Mixed 1.1 and 1.2 systems:
Set radio channel 1 to follow AFH on Piconet A, set radio channel 2 to follow Piconet A with basic hopping.

Use any synchronization mode to join piconet.

Scatter-Net tracing:
Set channel 1 to synchronise with Piconet A, set Channel 2 to synchronize with Piconet B.

Trace attempts of additional slave to join a Piconet (slave initiated):
Set Channel 1 to trace the piconet where the master has multiple slaves (sync and record is preferred with the master BD_addr). Set Channel 2 to have the joining slave as master and the established piconet master as the target (because the joining slave will make a temporary piconet with the master who will perform a master-slave switch to bring in the new slave). Use the page sync and record method on channel 2 and make sure the "show paging" traffic option is enabled.

UPF Time saver/Unknown master-slave roles:
Set channel 1 to synchronize with device A as master and device B as slave. Set Channel 2 to follow a separate piconet with Device B as master and Device A as slave. Start recording.
Regardless of which device initiates the connection, one of the radios will capture the piconet.