RS232 serial spy monitor cable

Introduction on monitoring serial RS232 data

The RS232 standard defines an asynchronous way of communication between DTE, data terminal equipment (computers, printers, etc.) and DCE, data communication equipment (modems). This type of communication has become the minority and nowadays serial communications is mainly between two DTE devices using a null modem cable. Although this is 1:1 communication, it is possible with special cables to monitor the data streams.

RS232 provides 2 data lines for each data channel. One is for transmitting data and the other for receiving. Because of these two separate lines, data can be send full duplex. This means that both ends can send and receive data simultaneously without mutual interference. In most situations however the high level communication protocol only allows half duplex communications because most simple protocols with external devices work with a master-slave, or question-answer configuration. One of the parties is the master which is in charge of communications. This master sends commands and requests to the slave which responds to them. The slave will never by itself start a communication sequence so in practise the communication is half duplex: There is no single moment when both sides send data simultaneously.

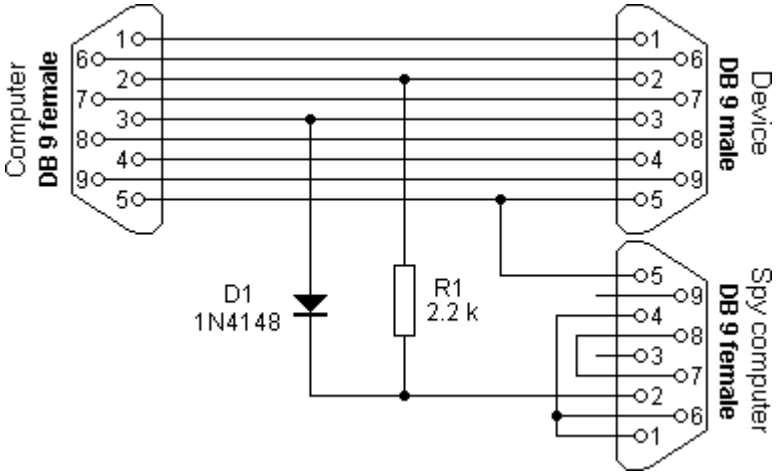
That most RS232 communication is performed in a half duplex way is important if the data stream has to be monitored. A half duplex communication protocol can be spied with a computer with just one serial port attached. This port listens to both RS232 communication lines simultaneously but no data will be garbled because only one party sends at a time. This type of communication can be spied with simple software like the terminal emulation program HyperTerminal which is shipped with the Windows operating system.

In the situation of full duplex communication on a RS232 channel we cannot simply tie both lines together and listen to it. For this situation you need two separate serial ports on the spionage computer. Also special sniffer software is handy that listens to both ports simultaneously and outputs the data of both lines to the screen or to disk.

Half duplex RS232 spy / monitor / sniffer cable

It is not difficult to monitor half duplex RS232 serial communication between two devices with a PC. To do this you need the RS232 monitor cable which is displayed in the next picture. Two DB9 connectors are wired straight through. The spy computer is connected to the third connector. This monitor cable taps communication from two sources on only one RS232 receiver port. This means that if the two devices happen to talk simultaneously, the monitored information will be garbage. In most circumstances communication protocols work half duplex, in which case this RS232 cable will work without problems. Otherwise you need the full duplex RS232 monitor cable which is discussed here also.

Half duplex RS232 spy / monitor / sniffer cable



Connector 1	Connector 2	Spy	Function
1	1	-	Carrier detect
2	2	2 via R_1	Rx → Rx_{spy}
3	3	2 via D_1	Tx → Rx_{spy}
4	4	-	Data terminal ready
5	5	5	Signal ground
6	6	-	Data set ready
7	7	-	Request to send
8	8	-	Clear to send
9	9	-	Ring indicator
-	-	1 + 4 + 6	DTR → CD + DSR
-	-	7 + 8	RTS → CTS

The electronic diagram looks simple and strange at the same time with one diode and one resistor. The functionality is however straight forward. The spy computer is attached to the connector in the right bottom. The female connector at the left is attached to the spied computer and the male connector at the right to the attached device.

When an **RS232** port is in an idle state, it will be in the so-called marking state with a negative voltage at the transmit output. Assume the computer connected to the left port is sending data and the peripheral device at the right side is idle. At that moment the RS232 signal level on line 3 will change. When the voltage of this line changes to a higher value, current will flow through the diode to the spy computer. We assume the attached device is in an idle state. Therefore, the voltage at line 2 is something like -12 Volt, while at the other end of the resistor +12 Volt is applied. Simple mathematics learns that a current of approximately 11 mA (=24 Volt/2200 Ohm) flows through the resistor. This is no problem because most RS232 driver IC's are capable to deliver at least 45 mA. Because the voltage drop over the diode is only 0.7 Volt—independent of the current through the diode—the spy computer will see on its RS232 port (almost) the same voltage levels as present on the transmit port of the sending computer and data from the sending computer to the peripheral device is successfully captured.

In the second situation the computer has finished sending data and waits for an answer from the device at the male connector. The RS232 signal level at line 2 will go to positive values. The diode will block current to line 3 so the spy computer effectively only sees the data coming from the peripheral device. Now the spy computer will be able to pick-up the data send from the device back to the computer.

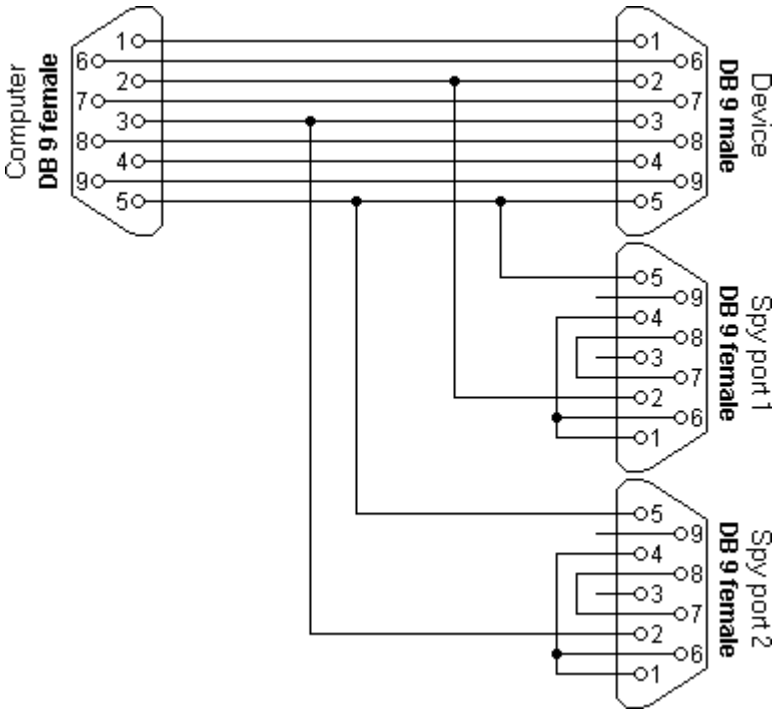
In the diagram for the half duplex monitor cable some shorts have been made between pins of the connector of the spying computer. These shorts loopback the handshaking signals of the computer. In most cases these shorts won't be necessary, but if the spy monitoring software uses handshaking, this will prevent the monitor software from blocking.

You don't need expensive software to use this RS232 spy cable. A simple serial terminal emulator like the HyperTerminal program present on all Windows based computers is enough to spy your communications. The only thing you need to do is changing the baudrate and start and stop bits settings from the terminal emulation program to the settings used on the line to monitor.

Full duplex RS232 spy / monitor / sniffer cable

As already discussed, it is not possible to monitor a full duplex RS232 communication with only one spy port. For this purpose the full duplex monitor cable can be used. This cable connects to two serial ports on the spy computer where each ports taps one direction of the communication. You could open two sessions of a terminal emulation program on your computer, but often better is to use one of the specialized RS232 monitor software products. In that way the two communication streams are merged in one screen which makes it easier to analyze the sequence of the communications.

Full duplex RS232 spy / monitor / sniffer cable



Connector 1	Connector 2	Spy port 1	Spy port 2	Description
1	1	-	-	Carrier detect
2	2	2	-	Rx → Rx_1
3	3	-	2	Tx → Rx_2
4	4	-	-	Data terminal ready
5	5	5	5	Signal ground
6	6	-	-	Data set ready
7	7	-	-	Request to send
8	8	-	-	Clear to send
9	9	-	-	Ring indicator
-	-	1 + 4 + 6	-	DTR → CD + DSR
-	-	7 + 8	-	RTS → CTS
-	-	-	1 + 4 + 6	DTR → CD + DSR
-	-	-	7 + 8	RTS → CTS

The diagram of the full duplex RS232 monitor cable is actually simpler than the diagram of the half duplex monitor cable. This is because no special circuitry is necessary to combine two communication lines on one input. Just to be sure, all handshake signals on both spy connectors have been looped back. This prevents the software from blocking input in case it checks the CTS, DSR or CD inputs.

Other RS232 monitor solutions

Besides the cables mentioned above, there are ready made adapters available on the market which monitor serial communications on RS232 channels. An interesting product is the EZ-Tap™ RS-232 Passive Tap Module from Stratus Engineering. It allows you to monitor RS232 communications via the USB port.