RS-232 Data Diode

Tutorial and Reference Manual

DRAFT

Douglas W. Jones
University of Iowa

July 28, 2006

Contents

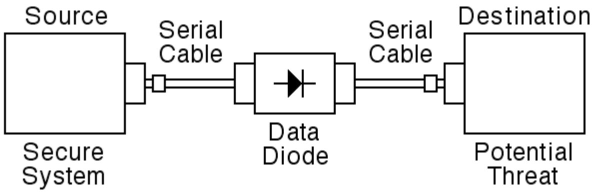
The current version of this document and related documents are available from
`http://www.cs.uiowa.edu/~jones/voting/diode/`

This documentation was developed at the University of Iowa with funds from the National Science Foundation under Grant No. CNS-052431 (ACCURATE) during 2006. Any opinions expressed here are those of the author and do not reflect the opinions of either the University of Iowa or the National Science Foundation.

Tom Bowersox actually built and tested the prototype RS-232 Data Diodes. His printed circuit board design was based on early drafts of this documentation, and the documentation was revised, when necessary, to reflect the results of his experiments.

Introduction

The RS-232 Data Diode allows one-way data flow from the serial port of one computer system to the serial port of another. This can be used, for example, to protect a secure source computer system from potential threats posed by an insecure destination system.



Use of the RS-232 Data Diode

If properly connected, the RS-232 Data Diode should be invisible to the software on the source and destination computer systems. As with any serial communications, the source and destination computer systems should be configured to use the same data rate, the same number of bits per character, and the same parity setting. We recommend the following for the serial data diode:

Data-rate: We have found that 1200 baud is reliable, and we have used rates up to 9600 baud. Experimentation is justified here, as the maximum baud rate depends, in part, on the cables you use.

Bits-per-character: This will usually be set to 8, to conform with the needs of most common character sets including Unicode encoded in UTF-8 format. It can be set to 7 for classic 7-bit ASCII.

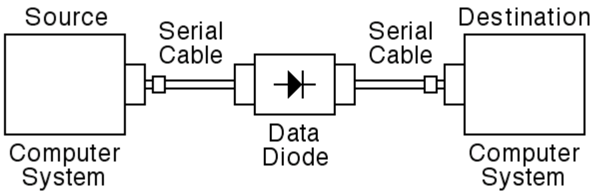
Parity: The usual options are mark, space, none, even and odd. Each of these may have some use. Because the RS-232 Data Diode does not support a reverse channel, and because opening the RS-232 Data Diode for inspection during use is normal and can cause transmission errors, we recommend using parity. For 8-bit data transmission, even and odd parity work equally well; for 7-bit data, odd parity is slightly better.

Because the RS-232 Data Diode has no reverse channel, there is no way for the receiver to signal that data has not been correctly received. Therefore, the higher level data should include provisions for forward error correction. The simplest approach to this has two components: First, each transmitted record should include a checksum of some kind so that the entire record can be discarded if it contains an error, and second, all records should be retransmitted many times.

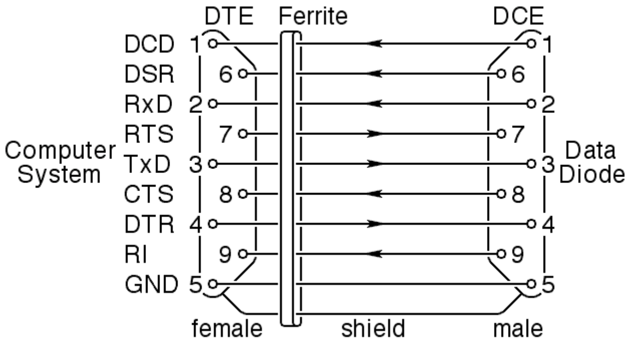
More complex error correcting codes may have some benefit in correcting single-bit errors, but remember that opening the cover on the data diode may cause signal dropouts that last for many record-times. Therefore, error correcting codes will not eliminate the need to retransmit all records periodically.

Cables

The RS-232 Data Diode allows one-way data flow from an RS-232 serial port of the source computer system to an RS-232 serial port of the destination computer system:



Each computer system sees the RS-232 Data Diode as a piece of data communications equipment (DCE). The serial ports of most computer systems conform to the standards for data terminal equipment (DTE). Therefore, the RS-232 Data Diode usually uses a pair of DCE to DTE cables. The most common cable, used with TIA 457 (IBM PC compatible) 9-pin serial ports, is wired as follows:



Note: All diagrams of cable connectors given here show the pinout as it appears when looking at the face of the connector from the outside.

This cable (or equivalent) is available from many sources. The connectors are commonly called DB9 connectors, and this cable is commonly called a straight-through DB9-male to DB9-female shielded cable.

The cable should be shielded. That is, the metal shells at each end of the cable should be connected by a shield conductor that encloses the others. This makes it hard to use the data lines as radio antennas. In addition, the metal shell of the connector on each computer should touch the computer's grounded metal frame, so that the shield itself does not serve as a useful antenna.

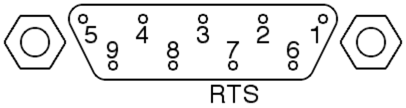
Another way to prevent the use of the cable's shield as an antenna is to use a cable that incorporates an integral ferrite bead around the cable at or very near the computer system end of the cable. Clip-on ferrite beads for this purpose are available.

Signal Definitions for the DB9 RS-232 Interface

Pin Number	*Name*	*Direction*	*Function*
1	DCD	DTE<DCE	Data Carrier Detect – some computer systems require this to be positive before data transmission.
2	RxD	DTE<DCE	Receive Data – data received by the computer system.
3	TxD	DTE>DCE	Transmit Data – data sent by the computer system.
4	DTR	DTE>DCE	Data Terminal Ready – the computer system should set this positive when it is ready to receive data.
5	GND		Signal Ground – the electrical return path for all signals; this line should not connect to the cable shield.
6	DSR	DTE<DCE	Data Set Ready – some computer systems require this signal to be positive before data transmission.
7	RTS	DTE>DCE	Request To Send – the computer system should set this positive prior to attempting to transmit data; the destination computer system should set this negative.
8	CTS	DTE<DCE	Clear To Send – some computer systems require this to be positive before data transmission.
9	RI	DTE<DCE	Ring Indicator – used only with modems; ignored by the RS-232 Data Diode and need not be connected.

Electrical Requirements

Before using the RS-232 Data Diode with a computer, it is appropriate to check that the serial port will work. First, measure the voltage between each pin on the DB9 serial port connectors and pin 5 (GND). None should be higher than 15 volts (positive or negative). Pins 3, 4 and 7 (TxD, DTR and RTS) should show at least 7 volts (positive or negative).

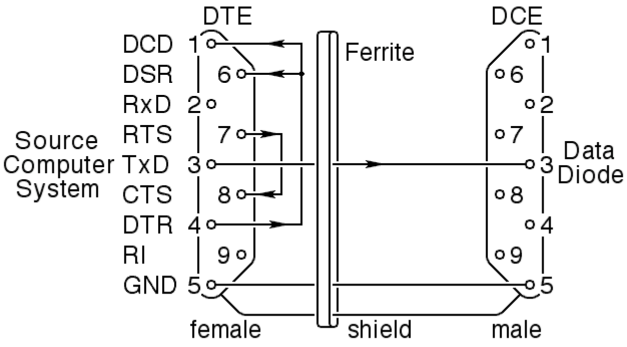


A few older computers used more than 15 volts. These may damage the RS-232 Data Diode. Some cheap computers have used voltages below 7 volts and may not work .

Second, measure the current from pins 3, 4 and 7 (TxD, DTR and RTS) to pin 5 (GND). If this is over 500 milliamps (positive or negative) the port is not RS-232 compliant. If it is below 20 milliamps, there may not be enough power for the RS-232 Data Diode.

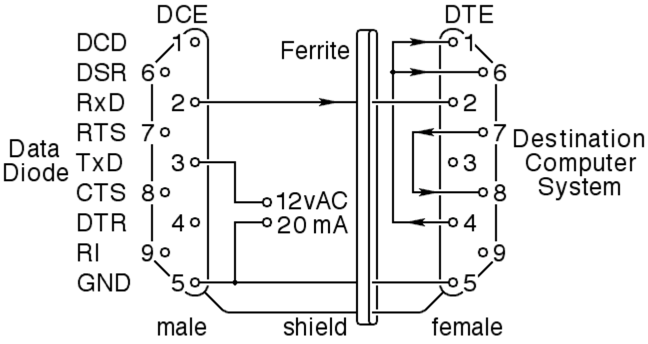
Alternative Cables

If the destination computer system cannot supply sufficient current on pins 3, 4 and 7 (TxD, DTR and RTS), or if it is desired to reduce the number of wires in the cables to prevent use of the extra wires to transmit covert data, alternative cables can be used.



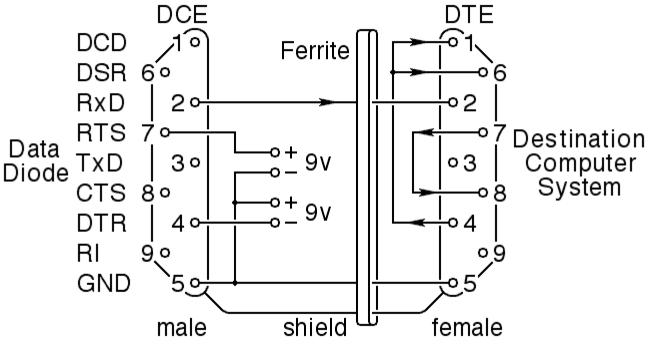
The alternative source cable has only two conductors inside the shield, TxD (pin 3) and GND (pin 5).

In addition, this cable includes loopback connections inside the shell of the connector to the source computer system. The RTS output from the source computer system (pin 7) is fed back into the CTS input (pin 8), and the DTR output (pin 4) is fed back into the DSR and DCD inputs (pins 1 and 6). These connections are identical to those established by a standard “loopback connector” used for serial port testing. A ferrite bead should be used at the computer end.



The alternative destination cable using AC power has only two conductors inside the shield, RxD (pin 2) and GND (pin 5).

This cable includes loopback connections inside the shell of the connector to the destination computer system. Power for the RS-232 Data Diode is provided through an auxiliary AC supply, typically a plug-in transformer. This provides power through TxD (pin 3) and GND (pin 5). Use of this power supply option may limit the data rate to 1200 baud. A ferrite bead should be used at the computer end.



The alternative destination cable using DC power is identical to the AC alternative, except for the power provisions.

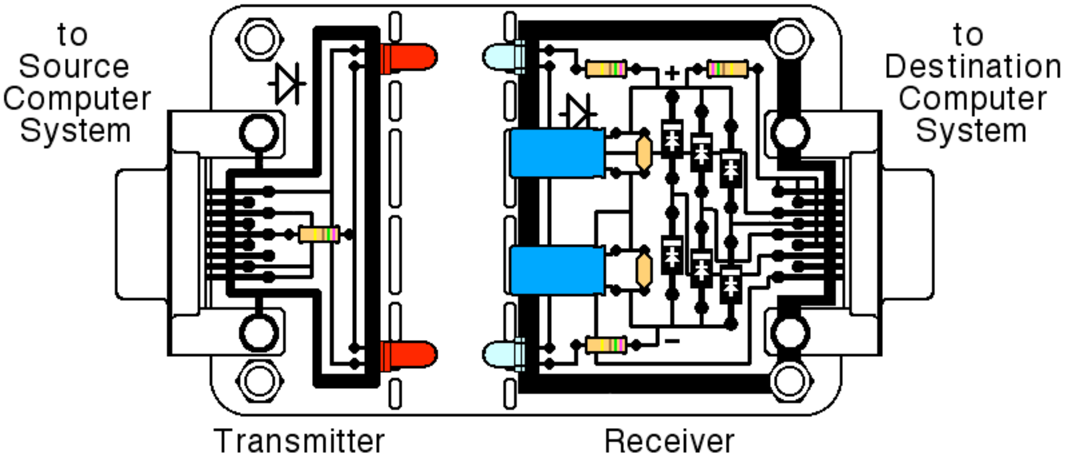
The DC cable includes connections for a pair of 9-volt DC supplies, typically 9-volt batteries. These provide positive power to RTS (pin 7) and negative power to DTR (pin 4), both relative to GND (pin 5). A ferrite bead should be used at the computer end.

Inside the RS-232 Data Diode

The cover on the RS-232 Data Diode is designed to be opened in order to allow easy inspection of the circuitry inside. This allows an outside observer to verify that the circuitry present performs only the authorized functions. By design, this circuitry avoids complex and difficult to understand components.

It is safe to open and inspect the RS-232 Data Diode in subdued light while data is being transmitted. It is also safe to unplug it for inspection and then re-attach it to the cables after inspection, even if data was being transmitted at the at the time. Obviously, opening or disconnecting the RS-232 Data Diode may introduce transmission errors, but all applications designed for use with any data diode must tolerate such errors by design.

The RS-232 Data Diode Consists of two halves, the transmitter and receiver. These are completely isolated from each other electrically. The transmitter is usually connected to the source computer system and is powered by it. The receiver is usually connected to the destination computer system and is powered by it.



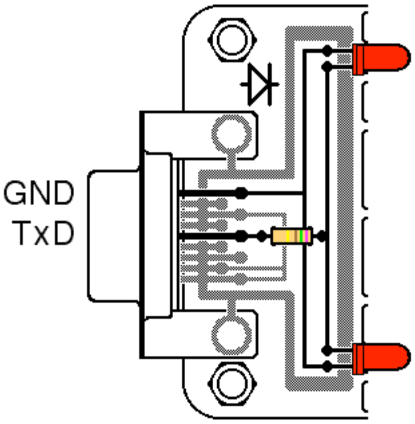
The transmitter converts electrical signals from the source computer system to optical form, using a pair of red LEDs. The receiver uses a pair of phototransistors to convert the optical data back to electrical form. The top LED/phototransistor pair transmits positive signals, while the bottom pair transmits negative signals.

The circuit board has wires printed on only one side. Removing it from the case and holding it up to a bright light should be sufficient to disclose that there are no hidden circuit traces buried inside the board. In normal use, one or the other of the LEDs should be on at all times, and when data is being transmitted, both LEDs should appear to be flickering. When the data line is idle, the bottom LED will be on solidly.

The data rate is limited by the impedance of the driven system (the cable plus the destination computer system itself). The primary limit on the baud rate is the gain of the phototransistors in the receiver.

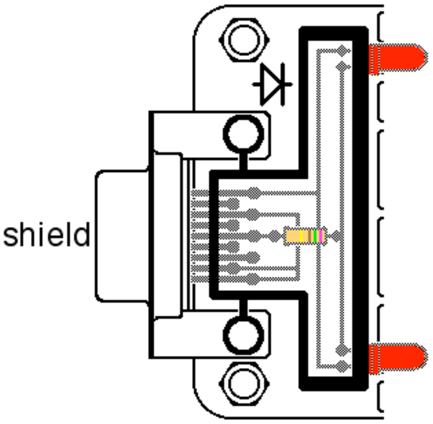
The RS-232 Data Diode Transmitter

There are three separate elements to the RS-232 Data Diode transmitter: The transmitter circuit, the shielding loop, and the loopback connections.



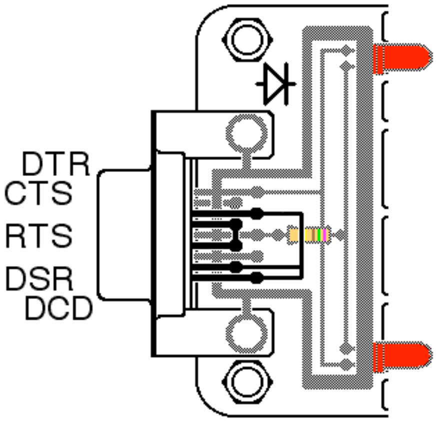
The transmitter circuit connects the TxD signal (pin 3) to GND, the signal ground (pin 5).

All of the power required to operate the transmitter is provided through the TxD line. When TxD is high (from 5 to 15 volts), current flows up through the top diode and resistor to make the top LED glow; when TXD is low (from -5 to -15 volts), current flows through the bottom diode and resistor, making the bottom LED glow. The resistor limits the current so that the LEDs will not burn out when connected to a computer that can drive more than 20 milliamps.



The shielding loop is a conductor that is tied to the shell of the cable connector, and through the cable connector to the shield of the cable.

This loop extends the cable shield in order to make it difficult for conductors inside the shield to act as antennas to transmit or receive signals from outside. The most significant potential antennas are the long vertical conductors between the two LEDs. Placing the shielding loop adjacent to these conductors significantly reduces their potential utility as antennas.

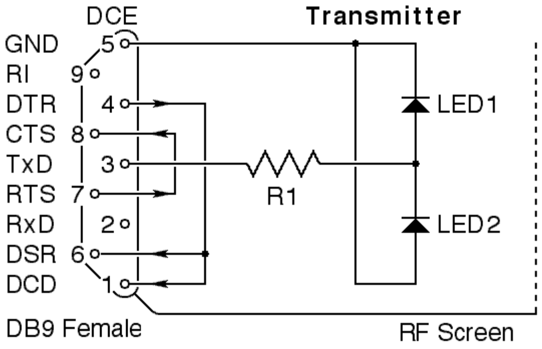


The loopback connections only matter if the cable to the source computer system includes connections for the DTR, CTS, RTS, DSR and DCD signals.

The RTS output from the source computer system (pin 7) is fed back into the CTS input (pin 8), and the DTR output (pin 4) is fed back into the DSR and DCD inputs (pins 1 and 6). These connections are identical to those established by a standard “loopback connector” used for serial port testing.

In the alternative cable suggested for connecting the source computer system to the RS-232 Data Diode, these “loopback” connections are wired inside the cable.

Transmitter Schematic and Parts List



LED1 and LED2 – Red LEDs with non-diffusing package with maximum current ratings of 20 milliamps, a nominal forward voltage drop of 2.2 volts, and a maximum reverse voltage greater than 3 volts. Panasonic LN28RCPP or LN28CPP should work. The non -diffusing package lowers the minimum operating voltage while making alignment between the transmitter's LEDs and the receiver's photodetectors somewhat critical.

R1 – 680 ohm ¼ watt resistor. For a maximum operating voltage of 15 volts and a maximum current of 20 milliamps through the LED, we use Ohm's law, with a current of .020 amps and 15 volts minus the forward voltage drop of the LEDs, 2.2 volts. This gives R1 = (15-2.2)/.020 = 640 ohms. We round this up to the nearest standard 5% resistor value, giving us 680 ohms. The power is (15-2.2)×.020 = 0.256 watts.

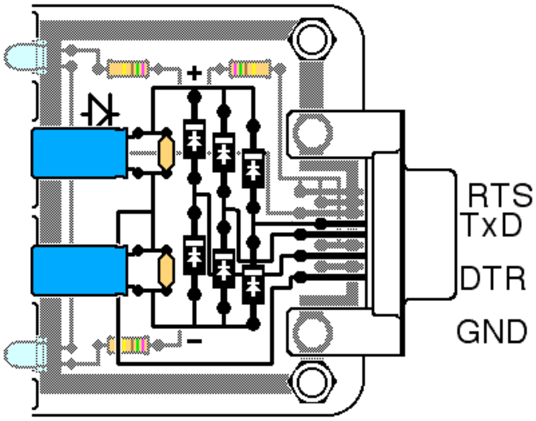
The RF screen for the transmitter consists of just the shielding loop around the transmitter circuit. It is not connected to the receiver or to the shielded enclosure. This not only prevents the creation of a ground loop, but it maintains complete electrical isolation between the transmitter and receiver.

The RS-232 Data Diode Receiver

There are four primary elements to the RS-232 Data Diode Receiver: The power supply, the receiver circuit, the shielding loop, and the loopback connections.

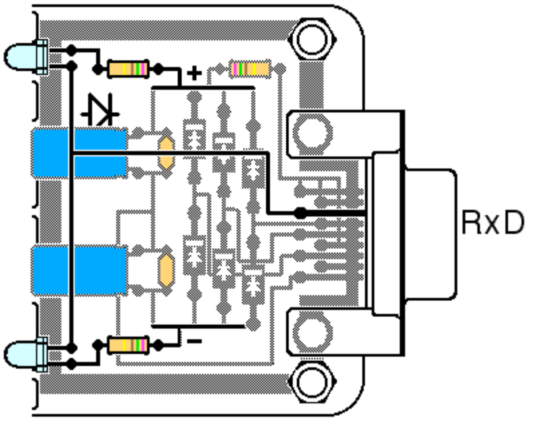
The power supply circuit takes power from RTS, TxD and/or DTR (pins 7, 3 and 4).

So long as one of these pins goes negative sufficiently frequently, the negative supply capacitors will remain charged between –7 and –15 volts. So long as one of these goes positive sufficiently frequently, the positive supply capacitors will remain charged between +7 and +15 volts. This allows for AC or DC power or for power from the destination computer system.



The receiver circuit uses the power supply to deliver a signal to RxD (pin 2).

When the top phototransistor is illuminated, it connects the positive supply to RxD through a resistor. When the bottom phototransistor is illuminated, it connects the negative supply to RxD through a resistor. The resistors prevent damage if both phototransistors are illuminated, for example, when the case is open so that room light falls on both phototransistors at once.

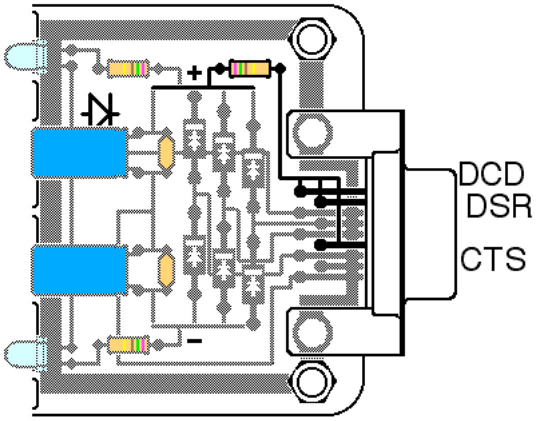


The shielding loop operates identically to that in the transmitter, except that it is also in electrical contact with the screws attaching the RS-232 Data Diode to its case.

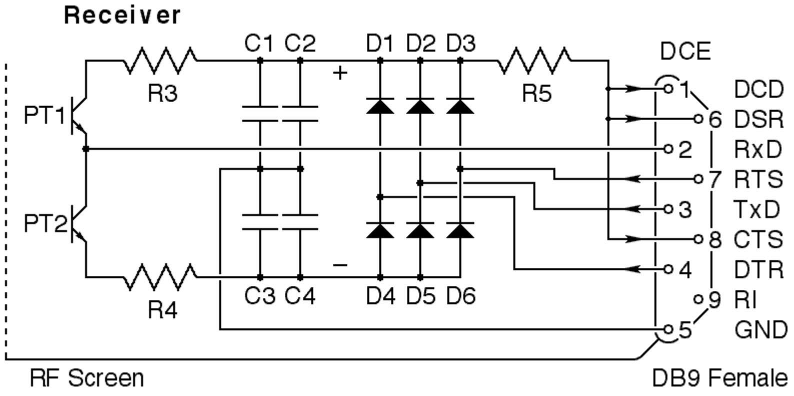
The loopback connections use the power supply to provide signals to DCD, DSR and CTS (pins 1, 6 and 8).

These signals are all set positive, indicating that the RS-232 Data Diode is operating.

In the alternative cables suggested for connecting the RS-232 Data Diode to the destination computer system, “loopback” connections are wired inside the cable.



Receiver Schematic and Parts List



PT1 and PT2 – NPN phototransistors; PNA1801LS, able to handle a maximum forward current of 20 milliamps and a forward voltage of 15 volts or more, with a collector current of at least 3mA at 500 Lux, peak sensitivity near 800nm, and a 4µs response time. Redesign with a transistor amplifier on each phototransistor should increase the data rate.

R1, R2 – 680 ohm ¼ watt resistors. To limit the phototransistor current to 20 milliamps at a maximum operating voltage of 15 volts, we use Ohm's law, with a current of .020 amps and 15 volts minus the forward voltage drop one diode, 0.6 volts. This gives R1 = (15-0.6)/.020 = 720 ohms. The nearest standard 5% resistor value is 750 ohms; 680 is a bit risky at 15 volts. The power is (15-0.6)×.020 = 0.288 watts. These resistors will rarely see this much power except when the case is opened in bright light.

R3 – 680 ohm 1/8 watt resistor. This limits the current to the handshaking pins, in the event of a short circuit. It is irrelevant if these signals are not used or are never shorted.

C1 and C3 – 100 microfarad 20 volt (or more) electrolytic capacitors. The worst case for the power supply is when 60 Hz AC power is used. We need to source 20 milliamps for 1/60th of a second (the interval between cycles on the power line). This is .02/60 = .00033 coulombs. 100 microfarads at 15 volts stores .0001×15 = .0015 coulombs. This gives us a factor of 5 safety margin, so the ripple under full load should be under 3 volts. Note that this full load condition will be rare.

C2, C4 – .01 microfarad 20 volt (or more) ceramic capacitors. The exact capacity is not critical. The primary purpose of these capacitors is to eliminate radio frequency interference from the RS-232 Data Diode power supply, and to filter out any radio frequency signals that might be injected into the Data Diode from its power supply connections. The larger capacitors C1 and C3 are electrolytic, and these typically do not do a good job of filtering out radio-frequency signals.

D1 through D6 – silicon diodes. 1N1001 diodes work well. These must be able to handle the inrush current during the charging of C1 and C3.

Intellectual Property Rights – Who owns the RS-232 Data Diode?

The RS-232 Data Diode was developed at the University of Iowa with funds from the National Science Foundation under Grant No. CNS-052431 (ACCURATE) during 2006.

U.S. Patent 5,703,562, *Method for transferring data from an unsecured computer to a secured computer*, granted Dec. 30, 1997 to Curt A. Nilsen, covers certain uses of the RS-232 Data Diode. Specifically, this patent applies to the use of this (and other) data diodes when the data transfer is from an insecure environment into a secure environment, which is to say, the data diode is used to block the export of data from the secure environment. This patent explicitly avoids claiming any rights over the use of data diodes for exporting data from a secure environment to an insecure environment, for example, where the data diode serves to prevent attacks against the secure system from the insecure system.

Data diodes and other devices for ensuring one-way flow of information have been around for a long time. U.S. Patent 5,206,368, *Signal isolating technique*, granted June 3, 1980 to Bruce N. Lenderking, covers use of optical isolators in high fanout signal distribution systems in order to prevent failures of one or another destination device from preventing delivery of the signal to other destination devices. In effect, this patent is the mirror of 5,703,562, since the signal source and all still-functional recipients are being secured against failures in one or more recipients. If malicious behavior is accepted as a type of failure, the expiration of this patent has expired may put most data diode applications in the public domain.

The Owl Computing Technologies data diode uses fiber optics and two specially configured ATM network interface cards. Inspection of this device to confirm that it is incapable of sending data in the reverse direction is not at all trivial. Most of the Owl data-diode documentation explicitly assumes the context of U.S. Patent 5,703,562, speaking in terms of using the data diode to assure that nothing escapes from the secure machine onto the Internet (`http://www.owlcti.com/products.htm`). It is noteworthy, however, that the final suggested application in the Owl application notes (`http://www.owlcti.com/applications.htm`) suggests using a data diode to deliver content to an insecure web server from a secure content provider. At the very least, this mention precludes anyone else patenting the use of Data Diodes for such a purpose.

The Tenex Datagate Interactive Link Data Diode (IL-DD) is also documented in terms of U.S. Patent 5,703,562 (`http://www.tenix.com/Main.asp?ID=734`). The documentation speaks in terms of using the data diode to send data from a network of uncertain security into a secure network Again, this device, although certified to a very high level of security, is an opaque device, forcing the user to trust the certifying agency.