

Receive only UTP cables

Diego González Gómez
<dggomez@users.sourceforge.net>

Text Last Updated: June, 2003

HTM Version Available¹

Abstract

One of the disadvantages of a sniffer is that it may be detected by other hosts. There are a number of methods to avoid detection, one being configuring the sniffer without an IP address. But none of them are as effective as the use of receive-only (sniffing) cables. These cables allow a sniffer to see network traffic without being detected by other hosts or an attacker. These cables therefore prove very useful in environments with Intrusion Detection Systems or honeypots (such as Honeynets).

Keywords: receive-only, cables, sniffing.

1 Introduction

There are several reasons to use a Network Sniffer. A Sniffer may be used to understand and fix problems in network traffic or to detect abnormal activities, and unfortunately one may also be used by an attacker to steal critical information.

The widespread use of NIDS (Network Intrusion Detection Systems) from the mid-1990s onwards, and the popularity of Honeynets in the last few years have increased the importance of sniffer user. Going forward, we will probably see sniffing tools play an increasingly important role in the future security of our networks.

Receive-only UTP (Unshielded Twisted Pair) cables are standard [RJ45] cables manually modified to allow only the data-receive signal. Therefore the sniffer communication capabilities are modified at the physical layer and for this reason are very effective. Further, it makes them very cheap and simple to build, plus their use has almost no impact on network performance.

In this article I will explain how to make these cables in a few easy steps and also discuss Network Taps briefly, which are alternatives "to make your own".

2 Fundamentals

2.1 Wiring schemes

As mentioned previously, this article is related to UTP cables, with RJ45 connectors. Before explaining the various sniffer types, it is necessary to understand the standard wiring schemes.

¹<http://www.dgonzalez.net/secinf/>

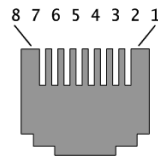


Figure 1: RJ45 connector.

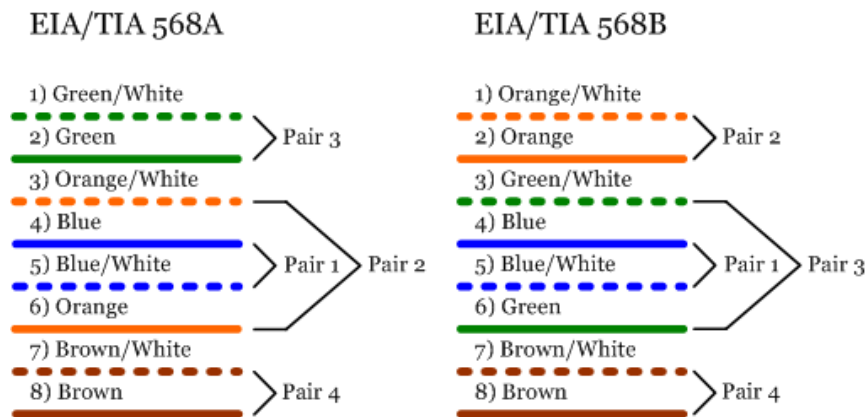


Figure 2: EIA/TIA 568A and 568B norms.

Figure 2 shows the pinouts.

Figure 3 describes what the wiring schemes are to make straight-through and crossover cables. To make a straight-through cable, the only important thing is to keep the wires in the same order in both ends.

2.2 Coding

It is important to understand the signals that travel through these cables. Ethernet LANs use digital signals to share data among network devices. Ethernet (but not Fast Ethernet) uses Manchester encoding to transmit the signal: transition occurs in the middle of each bit period. Two levels represent one bit. A low to high transition in the middle of the bit

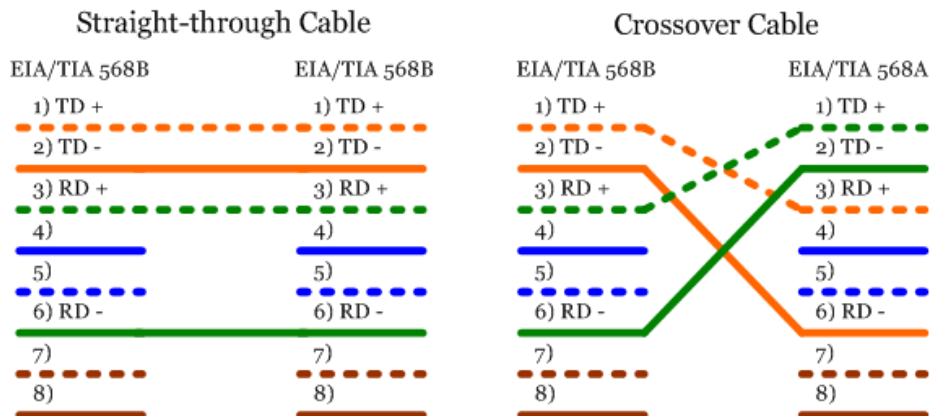


Figure 3: Straight-through and Crossover wiring schemes.

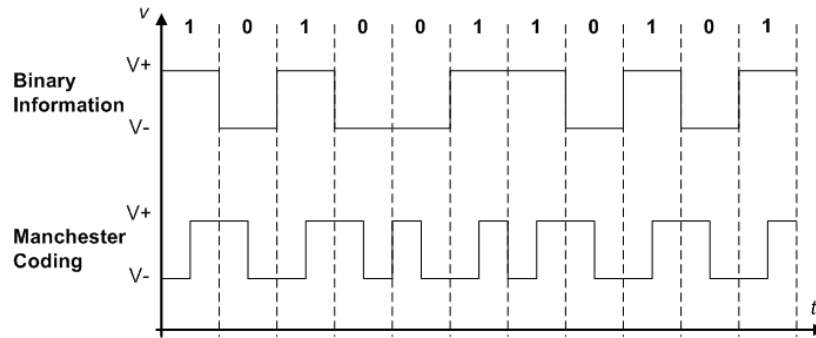


Figure 4: Manchester coding.

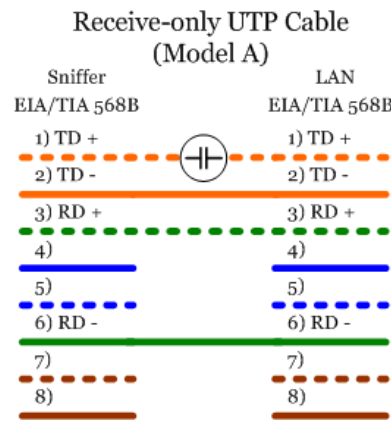


Figure 5: Model A wiring scheme.

represents a '1'. A high to low transition in the middle of the bit represents a '0'. There is no DC component. It uses positive/negative voltages.

3 Models

The goal of a receive-only UTP cable is to generate a lot of CRC errors on the sniffer's Transmit Data Signal. This avoids the remote device (hub, switch, router, etc.) recognizing any data sent by the sniffer, but keeps the link up.

In the following models, a few examples of sniffing-cable preparation are explained.

3.1 Model A

As we can see, this model uses an electronic component to insert high level of CRC errors. [1]

Capacitor acts as a high-pass filter. According to the Ethernet signal, the capacitor's pass band should be above 5Mhz frequency.

To determine the capacitor's value we use this formula:

$$f = \frac{1}{2\pi RC}$$

For 10Mb Ethernet, the frequency is of 5Mhz, and the resistance is $R = (R_{source} + R_{load}) = 200$. Therefore, the capacitor's value should be of 150p(F).

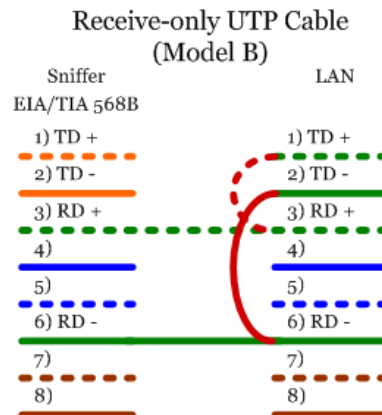


Figure 6: Model B wiring scheme.

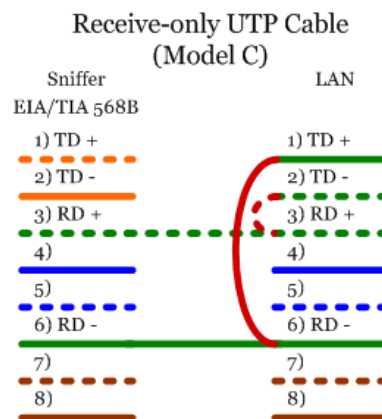


Figure 7: Model C wiring scheme.

For 100Mb Ethernet, the *frequency* is of 50Mhz, and the resistance is $R = (R_{source} + R_{load}) = 200$. Therefore, the capacitor should be of 15p(F).

This method introduces many CRC errors into the Transmit Data Signal maintaining the link up, but I have tried implementing it without success in a 10Mb Ethernet environment.

3.2 Model B

An easier way to implement a sniffer cable is by connecting pins 1 and 2 on the LAN side to its pins 3 and 6 on the remote side respectively. [2]

This method returns any signal sent from the LAN to itself, acting like a hub. Of course, it does not work with a switch, but that is not important, we will never plug a receive-only UTP cable into a switch, because we will only receive the traffic sent to the sniffer. If the switch has spanning ports, the situation is different. I have tested this model in my LAN, with a hub, and it works fine.

3.3 Model C

Model B can be improved just by changing the order of the connections.

Figure 7 describes the wiring schemes for Model C. If we connect pins 1 and 2 of the LAN

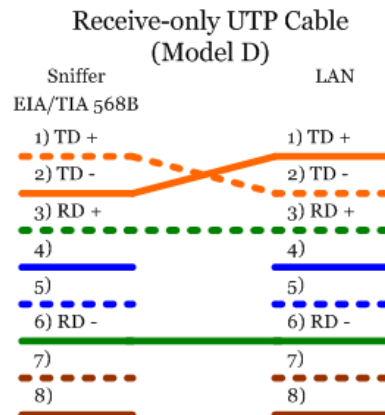


Figure 8: Model D wiring scheme.

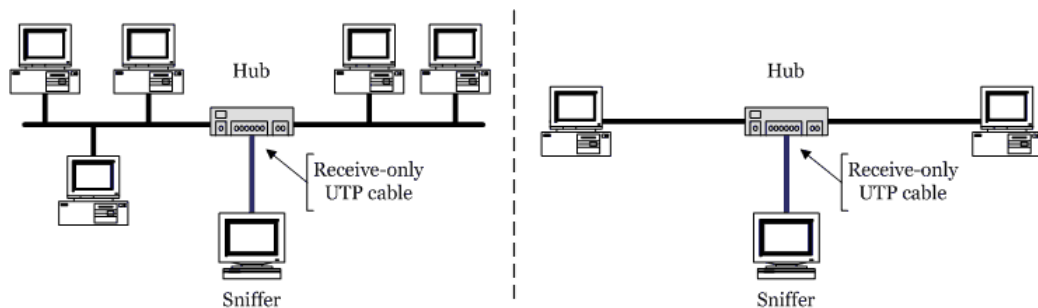


Figure 9: Intercepting communications with a hub and a sniffer cable.

side to pins 6 and 3 respectively, the signal returned to the LAN is inverted. This method ensures the link remains up and introduces a lot of errors on the sniffer cable's Transmit Signal. This model works as well as Model B on a hub. This is probably my favourite one because it modifies the signal returned to the LAN.

3.4 Model D

The last model is even easier than the three previous ones. It just changes the order of the Transmit Data Signal pins.

The signal sent from the sniffer is inverted, making it incomprehensible in the LAN side but ensuring that the link stays up. Unfortunately, I have implemented this model, but my hub surprisingly recognize the signal.

4 Implementation

These cables can be plugged into a hub to sniff all the traffic that passes through it. On the other hand, we can use a hub and sniffer-cable combination to intercept the communications between two network devices. Both situations are described in figure 9. It does not matter that the LAN is 10Base-T or 100Base-T if we use a hub that supports those speeds and we use the appropriate receive-only UTP cable model.

5 Network Taps

The alternative. Network Taps are commercial products that allow you to examine network traffic. A LAN Analyzer connected to a network tap for example, only receives data, so it does not disrupt any monitored communication.

Obviously, Network Taps are more expensive than making your own receive-only cables, but they are more robust and professional (we hope) and can monitor even fiber optic communications.

There are several companies that develop network taps. Shomiti Systems [3] and Net Optics, Inc. [4] [5] are two examples.

6 Conclusion

Receive-only UTP cables are a cheap and easy way to monitor SOHO. However, when the monitored network is greater, such as corporate networks that have large numbers of computers, then the need for professional devices that scale well will become obvious. In short, consider Network taps if you require advanced devices capable of monitoring high-speed connections.

The need to monitor and analyze network traffic has both increased the cost and returned greater value from network analysis. As is increasingly common in IT (Information Technology), each situation requires a different solution. I hope that this article offers the reader a few alternatives towards providing these solutions.

References

- [1] Sam Ng, *How to make a sniffing (receive-only) UTP cable*. 2001.
- [2] Holman, Paul. *OneWayEthernet*. Post to the ShmooGroup [online]. [cited 29 June 2003]. Available from: <<http://www.spack.org/index.cgi/OneWayEthernet>>
- [3] Shomiti Systems. *Network Analysis tools for Fast Ethernet, Switched Ethernet, Gigabit Ethernet, and other high speed LANs* [online]. [cited 29 June 2003]. Available from: <<http://www.shomiti.net/shomiti/century-tap.html>>
- [4] Net Optics, Inc. *Fast Ethernet Taps, Copper Network taps, 100 BaseT Tap for Analyzers and Probes* [online]. [cited 29 June 2003]. Available from: <<http://www.netoptics.com/net-96135.html>>
- [5] Net Optics, Inc. *Fast Ethernet Taps, Fiber Optic FX to TX tap, splitter, fast Ethernet or ATM, Fiber to Copper fiberoptic Splitter* [online]. [cited 29 June 2003]. Available from: <<http://www.netoptics.com/fx-tx-tap.html>>