Receive-only UTP cables and Network Taps

Diego González Gómez
diego (at) dgonzalez net

June, 2003
Text Last Updated: May, 2006

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 watch network traffic without being detected. Therefore they prove very useful in environments with Intrusion Detection Systems (IDS) or honeypot technologies (such as Honeynets).

Keywords: receive-only, cables, sniffing, network taps, uni-directional cables, span ports, mirror ports.

1 Introduction

A sniffer can be an excellent tool to understand and fix problems in network traffic, although 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. Nowadays, these tools play an increasingly important role in network security.

Receive-only (or uni-directional) UTP (Unshielded Twisted Pair) cables are standard (RJ45) cables manually modified to allow only the data-receive signal. Therefore, communication capabilities are modified at the physical layer and for this reason are very effective. Further, this solution is very cheap and simple to build, and since it does not interfere with traffic, it has no impact on network performance.

In this article I will explain how to build these cables in a few easy steps and also discuss Network Taps.

[1] http://www.dgonzalez.net

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 fundamental to understand the standard wiring schemes. Figure 2 shows the pinouts of a RJ45 connector.

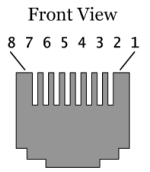

Figure 1: *Front view of a RJ45 connector*

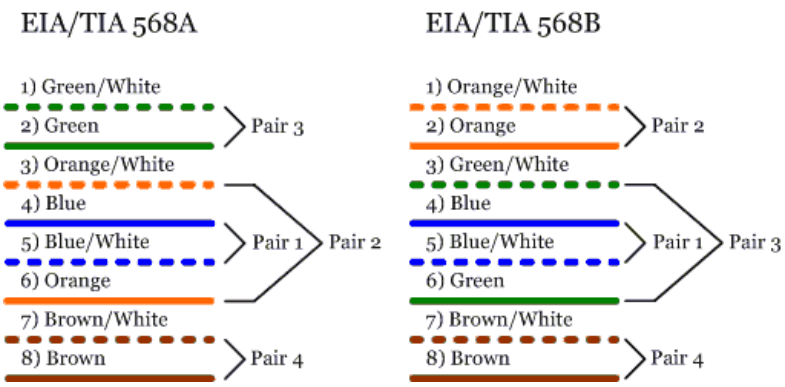

Figure 2: *EIA/TIA 568A and 568B norms*

Figure 3 describes the wiring schemes of straight through and crossover cables. Straight through cables can be used to connect a host or a router to a switch or hub. Crossover cables may be used to connect the following: host to host, hub to hub, switch to switch, switch to hub, router to router. The models of sniffing cables in this paper are based on straight through cables, but the crossover cables can be also used if the sniffer's transmit signal is modified in the same manner.

There are eight wires grouped into four coloured pairs. The pairs are twisted to reduce the effects of noise and interference. Each pair has a different twist ratio that can affect the signalling at higher speeds, so it becomes important to follow the colour codes. Note that pairs 1 (blue) and 4 (brown) are not used in 10Base-T or 100Base-TX Ethernet. All eight wires are used for 1000Base-T Ethernet. [1]

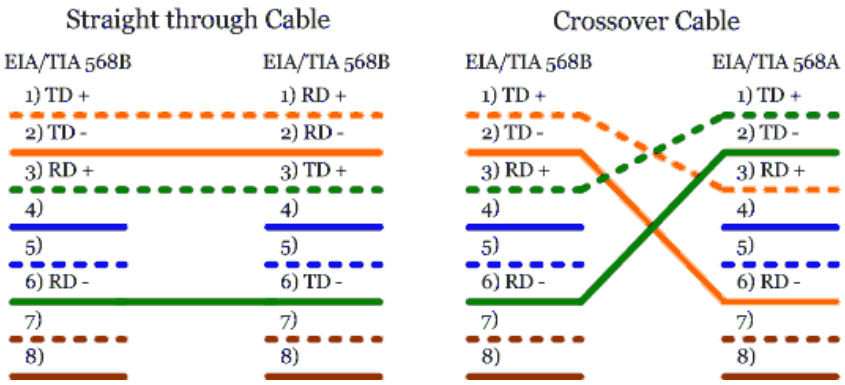

Figure 3: *Straight through and crossover wiring schemes (10/100Base-T)*

2.2 Coding

Ethernet LANs use digital signals to share data among network devices. 10Base-T 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 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.

100-BaseTX uses 4B/5B encoding, where each 4-bit nibbles is being transferred encoded as 5-bit symbols. The signalling model is a three level multi-level technique called MLT-3.

	10Base-T	**100Base-TX**
Data rate	10 Mbps	100 Mpbs
Encoding	Manchester	4B/5B
Signalling	5v. differential	MLT-3
Cable	Cat. 3 UTP	Cat. 5 UTP

Table 1: *Ethernet encoding and signalling*

3 Receive-only cables

3.1 Models

The goal of a receive-only UTP cable is to generate several errors on the sniffer's Transmit Data Signal. This avoids the remote device recognizing any data sent by the sniffer but at the same time keeping the link up.

In the following models, a few examples of sniffing-cable preparation are explained. All of these cable models are designed to work attached to a hub (half-duplex mode).

It is important to emphasize that these models are not designed to work with a switch because in working with a switch they will not be very useful. A switch

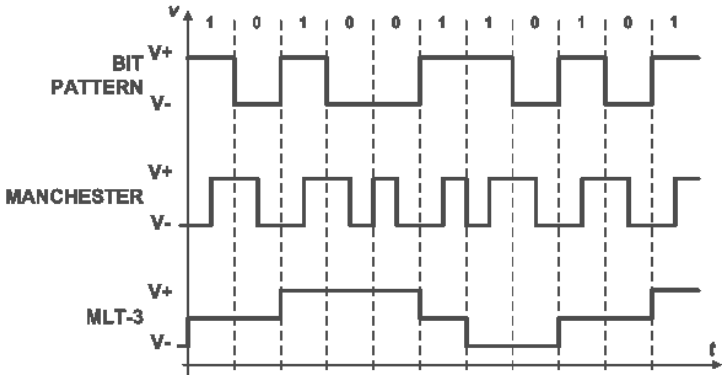

Figure 4: *Ethernet encoding schemes*

makes fowarding decisions using hardware addresses, and does not forward the traffic to all ports (unless it doesn't have the destination address in its switching table). It would require using ARP Spoofing techniques or something similar to intercept the conversations in the switch, and we would never receive all the traffic like we would with a hub. However, there are switches with span/mirror ports. These special ports receive the traffic of specified switch ports that the switch administrator nominates, acting like ports on a hub, but they can be overflowed if they receive more traffic than the one(s) they support. See section 4.2 'Taps vs. Span Ports' for more details.

3.1.1 Model A

As we can see, this model uses a capacitor to insert high levels of errors in the line. [2]

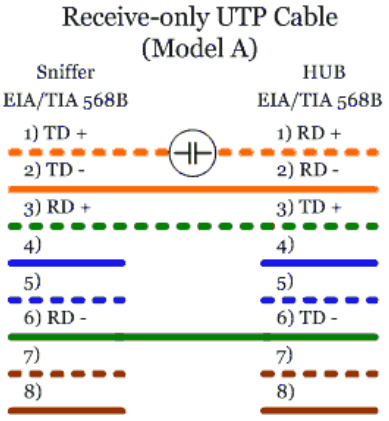

Figure 5: *Model A wiring scheme*

Capacitor acts as a high-pass filter. According to the 10Base-T signal, the capacitor's pass band should be above 5Mhz frequency. That is the minimum

frequency using Manchester encoding (with an alternate sequence with '0s' and '1s').

We can calculate the capacitor's value by the following method:

$$C = \frac{1}{2\pi Rf}$$

In a 10 Mbps Ethernet, the frequency is of 5Mhz, and the resistance is of R = *(Rsource+Rload) = 200* ohms. Therefore, the capacitor's value should be of 150p(F).

This method should introduce enough errors into the Transmit Data Signal, but keeping the link active at the same time. The figure 6 represents a simulation of the appearance of the output signal (blue, triangles), in relation to the original one (red, squares). The loose of power of the original signal, caused by the capacitor, can make it undetectable by the hub. Greater capacitors could be used to reduce this effect.

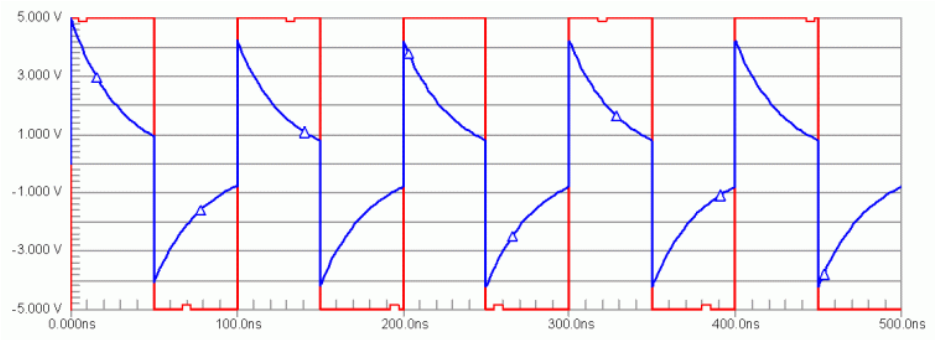

Figure 6: *Model A signal simulation*

I tried this model in an Ethernet LAN environment, attached to a 10/100 Mbps hub, but the link was not active.

3.1.2 Model B

An easier way to implement a sniffer cable is by connecting pins 1 and 2 (pair number 1) on the LAN side to pins 3 and 6 (pair number 2) on the same side respectively. [3]

This method returns any signal sent from the LAN to itself, acting like a hub. This model worked on a LAN with a 10/100 Mbps hub without problems.

3.1.3 Model C

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

Figure 8 describes the wiring schemes for Model C. If we connect pins 1 and 2 of the LAN side to pins 6 and 3 respectively, the signal returned to the LAN is inverted. This method ensures the link remains up and should introduce sufficient errors on the Transmit Signal to make it incomprehensible. As with

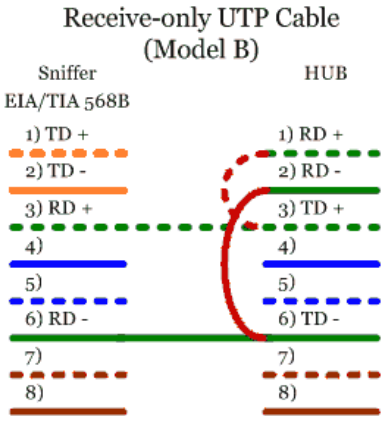

Figure 7: *Model B wiring scheme*

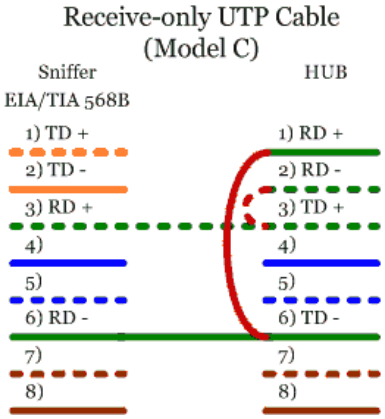

Figure 8: *Model C wiring scheme*

Model B, this model also works. However, this method is theoretically the best one because it modifies the signal returned to the LAN.

3.1.4 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 when received on the LAN side of the communication, but it ensures that the link stays up. Unfortunately, the hub used in the tests was able to recognize the signal sent by the sniffer.

3.2 Implementation examples

The typical scenario for using these cables is described in figure 10, plugged into a hub between the network segments to analyze. It does not matter that the

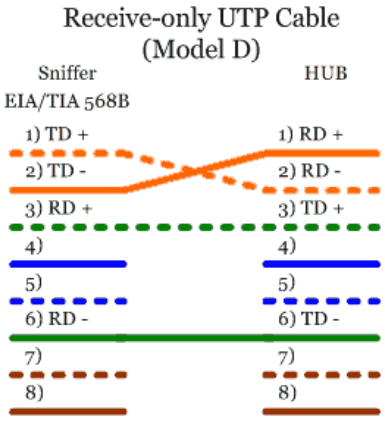

Figure 9: *Model D wiring scheme*

LAN is 10Base-T or 100Base-TX if we use a hub that supports the required speed. The disadvantage is that they can only work in half-duplex mode. In fact, the maximum efficiency of a hub is about 40% of the ideal speed.

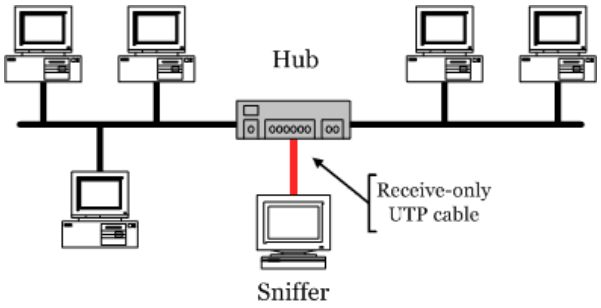

Figure 10: *Monitoring communications with a hub and a sniffer cable*

4 Network Taps

The alternative. TAP stands for Test Access Port. Network Taps are devices that allows to examine network traffic without causing any data stream interference. They work at OSI level 1, therefore they do not make any fowarding or routing decisions.

Obviously, Network Taps are more expensive than making your own receive-only cables, but they have more advantages. For example, they are more robust and professional, they usually have buffers to avoid data losses, they can monitor fiber optic communications, etc.

There are several companies that develop these products. Net Optics, Inc. [4], Shomiti Systems [5], Network Critical [6], Finisar [7], Intrusion Inc. [8], Datacom Systems Inc. [9] and Comcraft [10] are some of them.

It is interesting to note that all Tap manufacturers claim their copper Taps are fail-safe (no disruption to the link on powerloss). This is only partly true, because there is a 5-10 ms switchover time (a 0-1 packet loss possibility). In most environments this can be acceptable, but in a high availability network it can cause major issues such as causing the router and switches to renegotiate their links (VLAN, Spanning tree, etc). 4x4 Taps seems to be the only ones that offer 'zero' packet loss in the event of power-failure. Securicore [11] is one of the companies that distributes those Taps, from Network Critical.

Net Optics [4] offers PCI Network Taps for full-duplex monitoring access for 10/100 Mbps networks with a single NIC.

4.1 Schemes

The diagram 11 describes two ways to represent the Tap connection scheme.

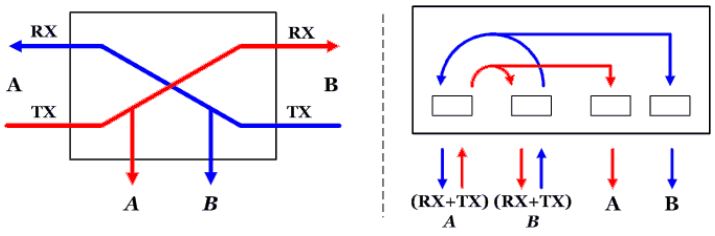

Figure 11: *TAP connection scheme*

A Tap captures network traffic in both directions and sends it to a monitoring device, such an IDS or a statistics traffic generator. As you can observe in figure 11, there is one data line by *each traffic direction*. Therefore, if we apply this scheme to UTP cables, which are usually used in Ethernet networks, we can easily deduce the following diagrams in figure 12.

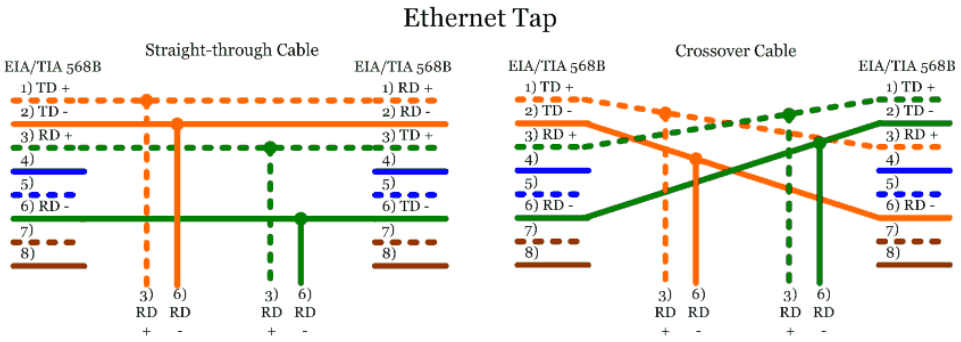

Figure 12: *Ethernet TAP connection diagrams*

To build a Tap like that is trivial. In fact, there are already instructions that explain how, with a straight through cable [12]. This solution requires two

network interfaces to analyze traffic (each one receives one direction). Keep in mind that the signal power of one network segment is not prepared to be shared by more than two network interfaces (source and destination). Therefore, this design can lead to signal (and data) losses.

More solutions for analyze traffic with Taps are discussed later on section 4.3 'Implementation Examples'.

4.1.1 Adaptive Taps

Adaptive Taps are designed to make signal conversions, in addition to capturing traffic. For example, there are Taps that convert signals from GigaBit-TX to Gibabit-SX, or from Gigabit-LX to Gigabit-SX.

4.1.2 Regeneration Taps

The idea of Regeneration Taps, from Net Optics [4], is to generate multiple streams of network traffic from a single access point. They act like several Taps combined in only one device, saving costs and space.

Regeneration Taps can be used in cases where it is necessary to analyze traffic in more than one way and with different machines. For example, both intrusion detection and protocol analysis may be used. Figure 13 represents this concept.

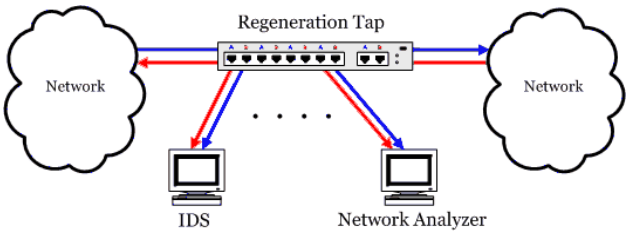

Figure 13: *Regeneration Tap*

Another way to implement a Regeneration Tap is using two or more Taps and sort them of daisy chain. 4x4 Critical Tap in figure 14 combines four individual Taps in one rackmountable case, and can be used in this manner. Although this can be done with both fiber and copper Taps, fiber Taps need more care with signal loss and must be ordered with the appropriate split ratio to preserve the live stream integrity.

4.1.3 Aggregation Taps

As we saw in figure 11, each traffic direction is a signal to analyze. Therefore, to monitor the traffic two network interfaces are needed. The advantage of the Aggregation Taps, among other features, is that they aggregate both signals into one, allowing the analysis with only one network interface. The Aggregation Tap by Network Critical [11] can, exceptionally, inject RESET TCP packets to kill hostile communications. This feature makes it especially useful in environments with NIDs with active response capabilities, or with NIPS (Network Intrusion Prevention Systems).

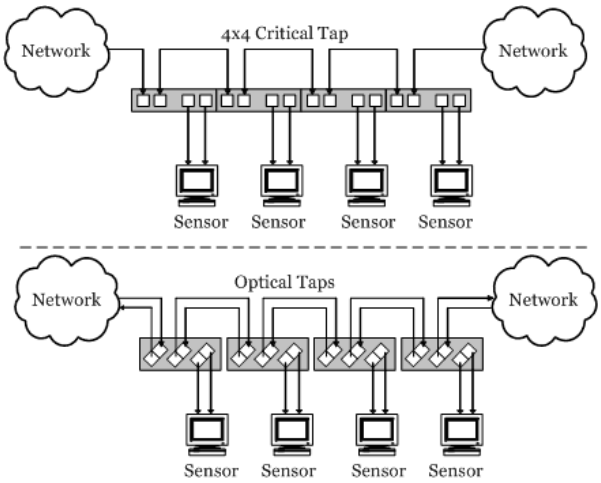

Figure 14: *Regeneration Tap using individual Taps*

4.2 Taps versus Span (mirror) Ports

Taps and span ports are used to monitor network traffic, but there are important differences between both technologies [14]:

1. **Traffic integrity.** The device connected to the Tap receives the same traffic as if it were also in-line, including all errors. See figure 15 for more details. Neither splitting nor regeneration introduce delay, or change the content or structure of information packets.

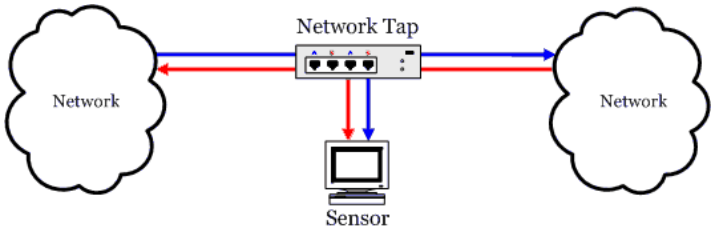

Figure 15: *Passive network monitoring*

On the other hand, a span port on a switch does not see all the traffic. Corrupt network packets, packets below minimum size, and layer 1 and 2 errors are usually dropped by the switch.

2. **Delay.** Taps pass full-duplex data at wire speed without affecting the actual traffic.

   By contrast, the software architecture of low-end switches introduces delay by copying the spanned packets. Worse yet, in many cases the data is being aggregated through a gigabit port, introducing a delay as the signal is converted from electrical to optical.

Furthermore, access to switch traffic is limited by the span port capacity. If the traffic passing through the span port is too great, the port will drop packets, thus some data loss will be experienced. For example, to see full-duplex traffic on each 100 Mbps link, a span port would need 200 Mbps of capacity.

3. **Resources.** Since Newtork Taps are passive devices, they can be left permanently in-line without affecting traffic.

   In contrast, span ports are apt to consume switch resources, degrading its overall performance.

4.3 Implementation Examples

There are many ways to implement network traffic analysis with Taps. The following are just a few of the methods available.

4.3.1 Sensor with two network interfaces

Figure 15 represents one way of analyzing traffic, using a sensor with two network interfaces, one for each traffic direction. In addition, some kind of software is required to aggregate the data from both physical interfaces into one logical interface. You can use for example the Sun Trunking software [13], or the Linux network bonding driver. The last option requires you to compile the driver *as a module* first, and then to combine the physical network interfaces into a logical one (`bond0`). For example, if we wish to bond the physical interfaces `eth1` and `eth2` to logical interface `bond0` with IP address 192.168.0.254/24:

```
[root@tap root]# modprobe bonding
[root@tap root]# ip addr add 192.168.0.254/24 brd + dev bond0
[root@tap root]# ifconfig eth1 promisc -arp up
[root@tap root]# ifconfig eth2 promisc -arp up
[root@tap root]# ifconfig bond0 promisc -arp up
[root@tap root]# ifenslave bond0 eth1
master has no hw address assigned; getting one from slave!
The interface eth1 is up, shutting it down it to enslave it.
[root@tap root]# ifenslave bond0 eth2
The interface eth2 is up, shutting it down it to enslave it.
[root@tap root]# ifconfig
bond0     Link encap:Ethernet  HWaddr XX:XX:XX:78:7F:C5
          inet addr:192.168.0.254  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING NOARP PROMISC MASTER MULTICAST  MTU:1500 Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:888 (888.0 b)  TX bytes:0 (0.0 b)

eth0      Link encap:Ethernet  HWaddr XX:XX:XX:77:02:13
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:151 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
```

```
          RX bytes:69180 (67.5 Kb)  TX bytes:17418 (17.0 Kb)
          Interrupt:11 Base address:0x3400

eth1      Link encap:Ethernet  HWaddr XX:XX:XX:78:7F:C5
          inet addr:192.168.0.254  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING NOARP PROMISC SLAVE MULTICAST  MTU:1500 Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:444 (444.0 b)  TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xd800

eth2      Link encap:Ethernet  HWaddr XX:XX:XX:78:7F:C5
          inet addr:192.168.0.254  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING NOARP PROMISC SLAVE MULTICAST  MTU:1500 Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:444 (444.0 b)  TX bytes:0 (0.0 b)
          Interrupt:11 Base address:0xd400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:18863 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18863 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1287600 (1.2 Mb)  TX bytes:1287600 (1.2 Mb)
```

Needless to say that ARP support is disabled since it is not needed by a receive-only device. As `bond0` is a logical interface, it can be used by `tcpdump`. The `eth0` interface can be used to remote control the sniffer, or to send alerts to a central console. More information on bonding can be found in `Documentation/networking/bonding.txt` file from the linux source code tree.

4.3.2 Using a switch span-port

On the other hand, if we have a switch with span ports, we can try the implementation of figure 16, from Jeff Nathan [15]. This implementation analyzes network traffic using a 100 Mbps or 1000 Mbps span port.

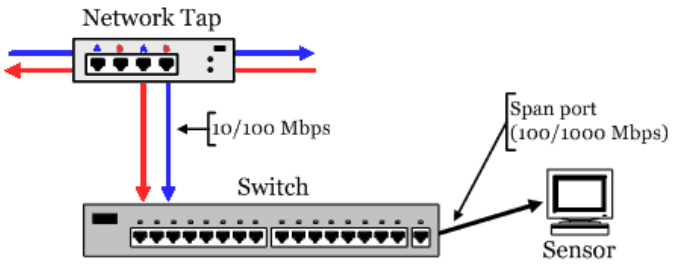

Figure 16: *Network Tap and switch with span port*

4.3.3 Load balancing. Multiple IDS

When monitoring high speed traffic (Gigabit fiber and higher) it becomes necessary to use multiple IDS systems and load balance between them. Figure 17 represents how to implement this type of configuration [16]. Netoptics also offers a detailed installation guide [17] for one of their Gigabit Fiber Taps.

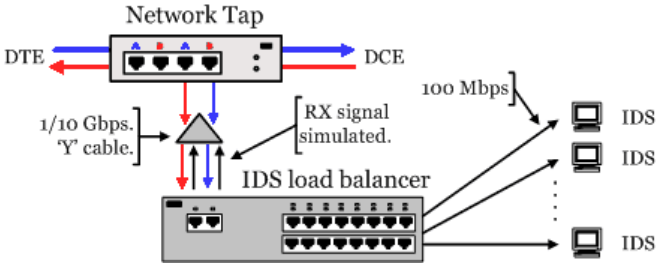

Figure 17: *High speed traffic analysis*

5 Conclusion

Receive-only UTP cables are a cheap and easy way to monitor home and SOHO LANs. However, when the monitored networks are greater in size, such as corporate networks that have large numbers of computers, professional devices that scale well are a better choice. 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 increased and will continue to rise going forward. This increase is due to both the need for improved network security and also the requirement to better understand our own IT infrastructures. As is in IT, each situation requires a different solution. I hope that this article has offered the reader a few alternatives suitable for their environment.

References

[1] Conectivity Knowledge Platform. *Ethernet (IEEE802.3)*. Post to the ShmooGroup [online]. [cited 20 May, 2005]. Available from: http://ckp.made-it.com/ieee8023.html

[2] Sam Ng, *How to make a sniffing (receive-only) UTP cable*, 2001. [online]. [cited 20 May, 2005]. Available from: http://www.geocities.com/samngms/sniffing_cable/.

[3] Holman, Paul. *OneWayEthernet*. Post to the ShmooGroup [online]. [cited 20 May, 2005]. Available from: http://www.spack.org/wiki/OneWayEthernet

[4] Net Optics, Inc. *Network Taps* [online]. [cited 20 May, 2005]. Available from: http://www.netoptics.com/products/default.asp

[5] Shomiti Systems. *Network Analysis tools for Fast Ethernet, Switched Ethernet, Gigabit Ethernet, and other high speed LANs* [online]. [cited 20 May, 2005]. Available from: http://www.shomiti.net/shomiti/century-tap.html

[6] Network Critical Solutions Limited *Critical TAPs* [online]. [cited 20 May, 2005]. Available from: http://www.criticaltap.com/products.asp

[7] Finisar. *Taps and Splitters* [online]. [cited 20 May, 2005]. Available from: http://www.finisar.com/nt/taps.php

[8] Intrusion, Inc. *SecureNet IDS Taps* [online]. [cited 20 May, 2005]. Available from: http://www.intrusion.com/Products/taps.asp

[9] Datacom Systems Inc. *Network Taps, Matrix Switches & Analyzers* [online]. [cited 20 May, 2005]. Available from: http://www.datacomsystems.com/solutions/overview.asp

[10] Comcraft *LAN & WAN Test equipment* [online]. [cited 20 May, 2005]. Available from: http://www.comcraftfr.com/

[11] Securicore Inc. *Critical Network Taps* [online]. [cited 20 May, 2005]. Available from: http://www.securicore.ca/critical_taps/

[12] Peters, Michael. *Construction and Use of a Passive Ethernet Tap* [online]. Jan, 2004 [cited 20 May, 2005]. Available from: http://www.snort.org/docs/tap/

[13] Sun. *Sun Trunking 1.3 Link Aggregation Software* [online]. [cited 20 May, 2005]. Available from: http://sun.systemnews.com/articles/66/2/sw/10639

[14] Net Optics, Inc. *Network Taps vs. Span Ports or Port Mirroring* [online]. [cited 20 May, 2005]. Available from: http://www.netoptics.com/products/pdf/taps-and-span-ports.pdf

[15] Nathan, Jeff. *100Mb IDS Tapping Diagram (with 1000bt span port)* [online]. [cited 20 May, 2005]. Available from: http://www.snort.org/docs/100Mb_tapping2.pdf

[16] Nathan, Jeff. *GIGE IDS Tapping Diagram (with load balancers)* [online]. [cited 20 May, 2005]. Available from: http://www.snort.org/docs/Gb_tapping.pdf

[17] Net Optics, Inc. *ATM Fiber Tap: Install guide* [online]. [cited 20 May, 2005]. Available from: http://www.netoptics.com/pdf/installation_guide/IGNET96042_142.pdf