Cables de sólo recepción y 'Network Taps'

Diego González Gómez
diego (at) dgonzalez net

Junio, 2003
Última actualización: Mayo de 2006

Resumen

Una de las desventajas de utilizar un 'sniffer' (rastreador) es que puede ser detectado por otras máquinas. Existen varias formas de evitar la detección, como configurar el rastreador sin una dirección IP. Sin embargo, ninguna de ellas es tan efectiva como el uso de cables de sólo recepción ('receive-only cables') o cables 'sniffing'. Estos cables permiten a un 'sniffer' monitorizar el tráfico de red sin ser detectado. Por ello, han demostrado ser especialmente útiles en entornos con Sistemas de Detección de Intrusiones (IDS), o tecnologías 'honeypots' (como las 'Honeynets' (Redes Trampa)).

Palabras clave: cables sólo recepción, rastreador, network taps, cables unidireccionales, sniffer, puertos span, puertos espejo.

1. Introducción

Un *sniffer* puede ser una excelente herramienta para comprender y solucionar problemas de tráfico de red, aunque también puede ser aprovechado por un atacante para robar información crítica.

El amplio uso de los NIDS (Sistemas de Detección de Intrusiones de red) desde mediados de los años noventa, y la creciente popularidad de las redes trampa han popularizado el uso de los *sniffers*. Actualmente, estas herramientas juegan cada vez un papel más importante en materia de seguridad de redes.

Los cables UTP (Par Trenzado no Apantallado) de sólo recepción (o unidireccionales) son cables RJ45 estándar modificados para permitir exclusivamente la señal de recepción de datos. De esta forma, las capacidades de comunicación se modifican en el nivel físico, razón por la que este método es tan efectivo. Además, esta solución es barata y fácil de construir, y al no interferir en el tráfico, no tiene impacto alguno sobre el rendimiento de la red.

En este artículo se explica cómo construir estos cables en pocos y sencillos pasos, y también se describen los *Network Taps* (dispositivos de escucha de red).

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

2. Fundamentos

2.1. Esquemas de cableado

Como ya se comentó, este artículo trata sobre cables UTP, con conectores RJ45. Antes de explicar los diferentes modelos, es fundamental comprender los esquemas de cableado estándares. La figura 2 ilustra los patillajes de un conector RJ45.

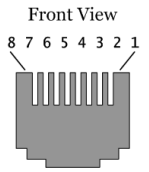

Figura 1: *Vista frontal de un conector RJ45*

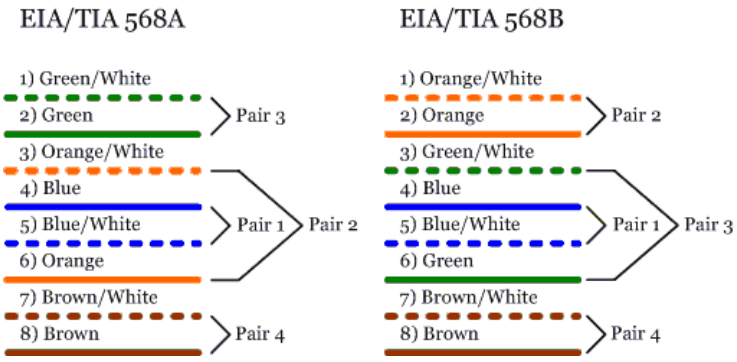

Figura 2: *Normas EIA/TIA 568A y 568B*

La figura 3 describe qué esquemas de cableado son necesarios para hacer cables directos (*straight through*) y cruzados (*crossover*). Los cables directos pueden ser utilizados para conectar un PC o un *router* a un *switch* (conmutador) o *hub* (concentrador). Los cables cruzados se utilizan para conectar: PC a PC, concentrador a concentrador, conmutador a conmutador, conmutador a concentrador, *router* a *router*. Los modelos de cables de sólo recepción de este documento están basados en cables directos, pero también se pueden utilizar cables cruzados siempre que la señal de transmisión del *sniffer* sea modificada de la misma forma.

Hay ocho cables agrupados en cuatro pares, según colores. Los pares están trenzados para limitar los efectos del ruido e interferencias. Cada par tiene un nivel de trenzado diferente que puede afectar a la señalización en altas velocidades, así que es importante respetar los códigos de colores. Nótese que los pares 1 (azul) y 4 (marrón) no son utilizados en Ethernet 10/100Base-T. Los ocho cables son utilizados en Ethernet 1000Base-T. [1]

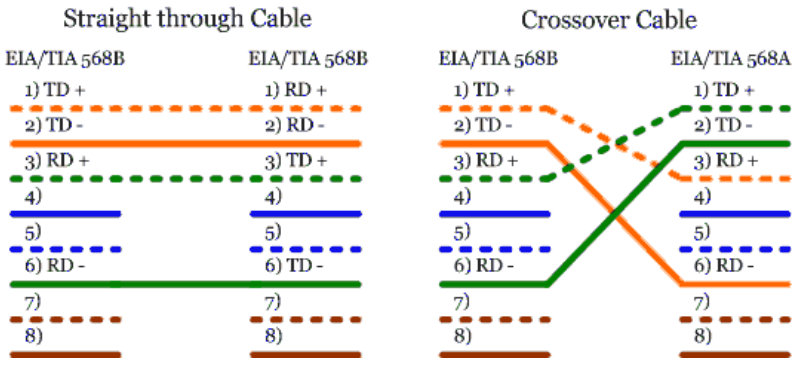

Figura 3: *Esquemas de cableado para cables directos y cruzados (10/100Base-T)*

2.2. Codificación

Las Ethernet LANs (Redes de área local Ethernet) utilizan señales digitales para enviar datos entre dispositivos de red. 10Base-T utiliza codificación Manchester para la transmisión de las señales: la transición ocurre en la mitad de cada período de bit. Dos niveles representan un bit. Una transición bajo alto a la mitad del bit representa un '1'. Una transición alto bajo a la mitad del bit representa un '0'. No existe componente continua (DC). Utiliza voltajes positivos y negativos.

100-BaseTX utiliza codificación 4B/5B, donde cada conjunto de 4 bits (*nibble*) se transmite codificado como símbolos de 5 bits. El modelo de señalización consiste en una técnica multinivel de tres niveles denominada MLT-3. La figura 4 ilustra algunos ejemplos de codificaciones.

	10Base-T	**100Base-TX**
Tasa transferencia	10 Mbps	100 Mpbs
Codificación	Manchester	4B/5B
Señalización	Dif. 5v	MLT-3
Cable	Cat. 3 UTP	Cat. 5 UTP

Cuadro 1: *Codificaciones y señalizaciones Ethernet*

3. Cables de sólo-recepción

3.1. Modelos

El objetivo de un cable UTP de sólo recepción consiste en introducir errores en la señal de transmisión de datos del *sniffer*. Esto evita que el dispositivo conectado pueda reconocer cualquier dato enviado por el *sniffer* manteniendo, sin embargo, el enlace activo.

A continuación se explican algunos modelos de cables UTP de sólo recepción o *sniffing-cable* (cable de rastreo). Todos estos cables están diseñados para funcionar con un concentrador (modo *half-duplex*).

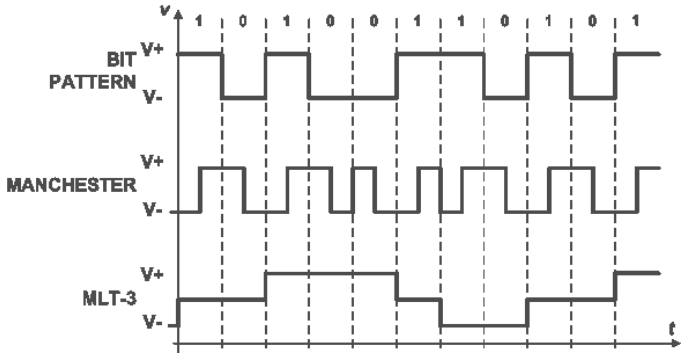

Figura 4: *Codificaciones Ethernet*

Es importante resaltar que estos modelos no están diseñados para funcionar con conmutadores porque en ese caso no serían de gran utilidad. Un conmutador toma decisiones de reenvío utilizando direcciones hardware, y no redirige el tráfico a todos los puertos (salvo cuando carece de la dirección de destino en su tabla de direcciones). Habría que utilizar técnicas de *ARP spoofing* (falseamiento de dirección ARP) o similares para poder interceptar otras conversaciones en un conmutador, y nunca recibiríamos todo el tráfico como con un concentrador. No obstante, existen conmutadores con puertos *span/mirror* (espejo). Estos puertos especiales reciben una copia del tráfico de determinados puertos del conmutador, de forma similar a como ocurre en un concentrador, pero pueden desbordarse si reciben más tráfico del que soportan. Lea el apartado 4.2 'Taps frente a puertos *span*', para más detalles.

3.1.1. Modelo A

Como se puede observar, este modelo utiliza un componente electrónico para introducir un alto nivel de errores en la línea. [2]

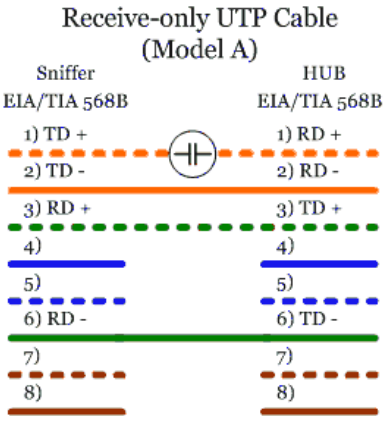

Figura 5: *Esquema de cableado del modelo A*

El condensador actúa como un filtro paso-alto. De acuerdo con la señal 10Base-T, la frecuencia de corte del filtro debería estar sobre los 5Mhz. Esta es la mínima frecuencia obtenida utilizando la codificación Manchester (con una secuencia alternada de '0s' y '1s').

Podemos determinar el valor del condensador de la siguiente forma:

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

En una Ethernet de 10 Mbps, la frecuencia es de 5Mhz. La resistencia es de $R = (Rsource+Rload) = 200$ ohms. Por lo tanto, el valor del condensador debería ser de 150p(F).

Este método debería introducir suficientes errores en la señal de transmisión, manteniendo al mismo tiempo el enlace activo. La figura 6 representa una simulación del aspecto aproximado que tendría la señal de salida (en color azul, con triángulos), con respecto a la original (rojo, con cuadrados). Las pérdidas de potencia de la señal original, provocadas por el condensador, pueden hacer que no sea detectada por el concentrador. Se podrían utilizar condensadores de mayor capacidad para reducir este efecto.

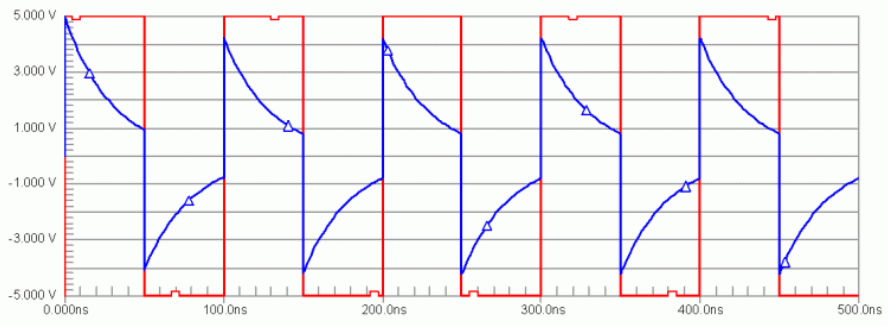

Figura 6: *Simulación de señales en el modelo A*

1 He probado este modelo en una LAN Ethernet, enchufado a un concentrador de 10/100 Mbps, pero el enlace no se mantuvo activo.

3.1.2. Modelo B

Una forma más sencilla de hacer un cable de sólo recepción consiste en conectar los pines 1 y 2 (par número 1) del lado de la LAN a los pines 3 y 6 (par número 2) del mismo lado respectivamente. [3]

Este método devuelve cualquier señal enviada desde la LAN a sí misma, actuando como un concentrador. Este modelo funcionó con un un concentrador de 10/100 Mbps sin problemas.

3.1.3. Modelo C

El modelo B puede ser mejorado con tan sólo cambiar el orden de las conexiones.

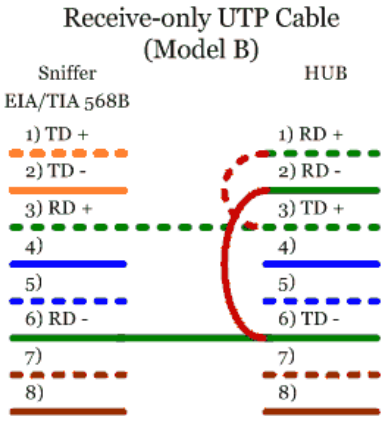

Figura 7: *Esquema de cableado del modelo B*

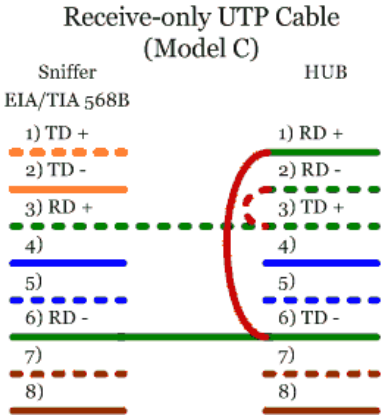

Figura 8: *Esquema de cableado del modelo C*

La figura 8 describe el esquema de cableado para el modelo C. Si conectamos los pines 1 y 2 del lado de la LAN a los pines 6 y 3 respectivamente, la señal devuelta a la LAN está invertida. Este método asegura que el enlace esté activo y debería introducir suficientes errores en la señal de transmisión como para hacerla incomprensible. Como el modelo B, este modelo también funciona. Sin embargo, este método es teóricamente mejor ya que modifica la señal devuelta a la LAN.

3.1.4. Modelo D

El último modelo es incluso más sencillo que los tres anteriores. Simplemente invierte el orden de los pines de la señal de transmisión de datos.

La seal enviada desde el *sniffer* está invertida, haciéndola incomprensible al extremo de la LAN pero asegurando que el enlace permanece activo. Por desgracia, el concentrador utilizado en las pruebas fue capaz de reconocer la

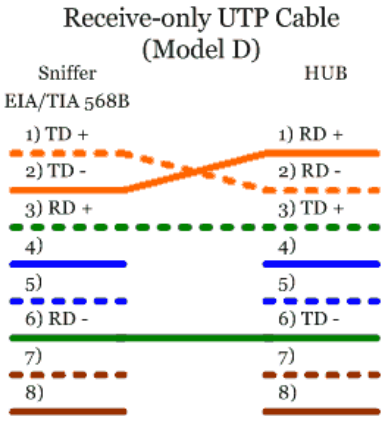

Figura 9: *Esquema de cableado del modelo D*

señal enviada por el *sniffer*.

3.2. Ejemplos de implementación

El escenario típico para el uso de estos cables es descrito en la figura 10, conectados a un concentrador por el que circula el tráfico a analizar. No importa si la LAN es 10Base-T o 100Base-TX, siempre que utilicemos un concentrador que soporte la velocidad requerida. El mayor inconveniente es que sólo pueden trabajar en modo *half-duplex*. De hecho, el máximo rendimiento de un concentrador está en torno al 40 % de la velocidad ideal.

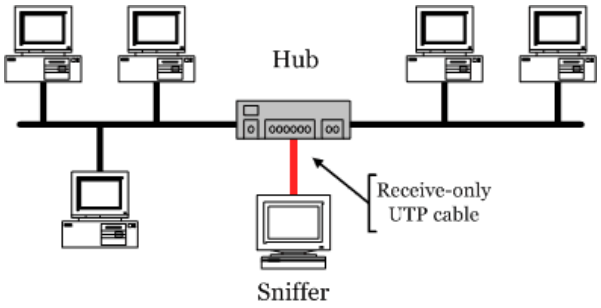

Figura 10: *Monitorización con concentrador y cable de sólo recepción*

4. 'Network Taps'

La alternativa. TAP significa 'Test Access Port' (Puerto de Acceso de Pruebas). Los Network Taps (dispositivos de escucha de red) son dispositivos que permiten examinar el tráfico de red sin intervenir en el flujo de datos. Trabajan a nivel 1 de OSI, por lo que no realizan ninguna función de redirección o encaminamiento del tráfico.

Obviamente, los Network Taps son una solución más costosa que los cables UTP de sólo recepción, pero cuentan con muchas más ventajas. Por ejemplo, son más robustos y profesionales, suelen tener búfers para evitar pérdidas de datos, regeneran la señal, pueden monitorizar comunicaciones de fibra óptica, etc.

Hay varias compañías que desarrollan estos productos. Net Optics, Inc. [4], Shomiti Systems [5], Network Critical [6], Finisar [7], Intrusion Inc. [8], Datacom Systems Inc. [9], Comcraft [10] son algunas de ellas.

Es interesante mencionar que todos los fabricantes de Taps afirman que sus productos son seguros ante fallos (el enlace no se interrumpe con pérdidas de tensión). Esto es sólo parcialmente cierto, ya que existe un período de intercambio de entre 5 y 10 ms (una probabilidad de pérdida de 0 ó 1 paquetes). En la mayoría de los entornos esto puede ser aceptable, pero en una red de alta disponibilidad puede provocar efectos importantes como la renegociación de los enlaces entre *routers* y switches (VPN, Spanning tree, etc.) Al parecer, los 4x4 Taps son los únicos que ofrecen 'cero' pérdidas de paquetes ante fallos de alimentación. Securicore [11] es una de las compañías que distribuye estos Taps, desarrollados por Network Critical.

Net Optics [4] ofrece Network Taps PCI para la monitorización full-duplex de redes 10/100 Mbps a través de una única interfaz de red (NIC).

4.1. Esquemas

El diagrama 11 describe dos formas de representar el esquema de conexiones de un Tap.

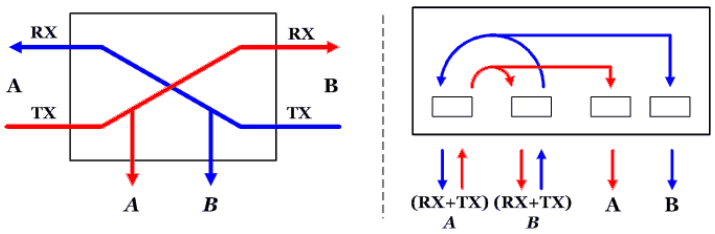

Figura 11: *Esquema de conexiones de un TAP*

Un Tap captura el tráfico en ambos sentidos y lo envía a un dispositivo de monitorización, como un IDS o un generador de estadísticas de tráfico. Como se puede observar en la figura 11, se obtiene una línea de datos por *cada sentido* del tráfico. Por lo tanto, si aplicamos este esquema de conexiones a cables UTP, que son los que normalmente se utilizan en redes Ethernet, podemos deducir fácilmente los esquemas de la figura 12.

Construir un Tap de estas características es trivial. De hecho, ya existen instrucciones que indican cómo hacerlo, con un cable directo [12]. Esta solución requiere dos interfaces de red para analizar el tráfico (cada una recibe un sentido de la comunicación). Tenga presente que la potencia de la señal de un segmento de red no está preparada para ser compartida por más de dos interfaces de red (origen y destino). Por lo tanto, este diseño puede provocar pérdidas de señal (y de datos).

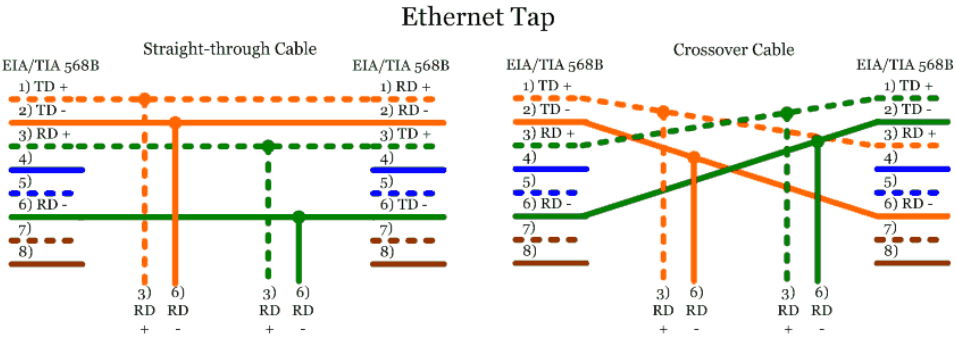

Figura 12: *Esquemas de conexiones para TAPs Ethernet*

Otras soluciones para analizar el tráfico con Taps se comentan más adelante en el apartado 4.3 'Ejemplos de Implementación'.

4.1.1. Taps de adaptación

Los Taps de adaptación ('Adaptive taps') están diseñados para hacer conversiones de señales, además de capturar tráfico. Por ejemplo, existen Taps que convierten señales de Gibabit-TX a Gibabit-SX, o de Gigabit-LX a Gigabit-SX.

4.1.2. Taps de regeneración

La idea de los Taps de regeneración ('Regeneration Taps'), de Net Optics [4], consiste en generar múltiples flujos de tráficos de red a partir de un único punto de acceso. Actúan como varios Taps combinados en un sólo dispositivo, ahorrando en costes y espacio.

Los Taps de regeneración pueden ser utilizados en casos donde es necesario analizar tráfico de más de una forma y con diferentes máquinas. Por ejemplo, se podría llevar a cabo detección de intrusiones y análisis de protocolo. La figura 13 ilustra este concepto.

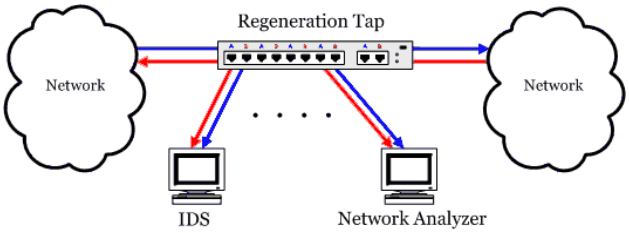

Figura 13: *Tap de regeneración*

Otra forma de implementar un Tap de regeneración es utilizando dos o más Taps y disponerlos en una *daisy-chain* (cadena de margarita). El *4x4 Critical Tap* en la figura 14 combina cuatro Taps individuales, y puede ser utilizado

de esta forma. Aunque es posible hacer esto tanto con Taps de fibra o cobre, los Taps de fibra necesitan más cuidados con la pérdida de señal y deben ser ordenados según la relación de separación (*split ratio*) adecuada para preservar la integridad del flujo de datos.

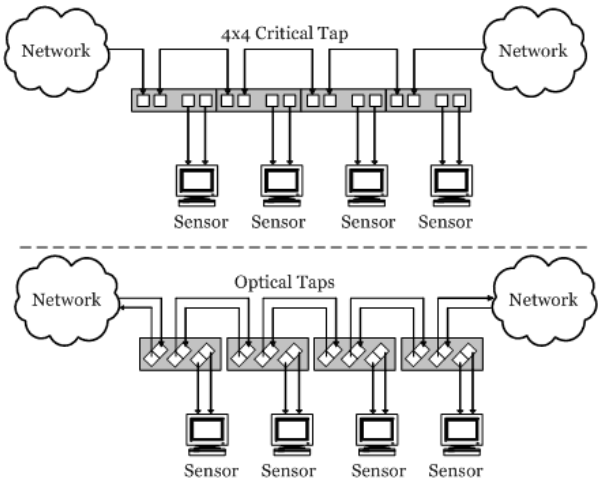

Figura 14: *Taps de regeneración mediante Taps individuales*

4.1.3. Taps de agregación

Como vimos en la figura 11, cada sentido del tráfico es una señal de datos que hay que analizar. Por lo tanto, para poder monitorizar el tráfico de red es necesario tener dos interfaces de red. La novedad de estos Taps ('Aggregation Taps') ente otras características, es que reunen ambas señales de datos en una sola, permitiendo el análisis mediante una única interfaz de red. El Aggregation-TAP de Network Critical [11] permite además, de forma excepcional, inyectar paquetes TCP RESET en la red, eliminando aquellas conexiones que pueden ser hostiles. Esta característica lo hace especialmente útil en escenarios con NIDSs con capacidades de respuesta activa, o NIPSs (Sistemas de Prevención de Intrusiones).

4.2. Taps frente a puertos *span* (espejo)

Los puertos de un Tap y los puertos *span* de un conmutador se utilizan para monitorizar tráfico de red, pero hay diferencias importantes entre ambas tecnologías [14]:

1. **Integridad del tráfico:** El dispositivo conectado al Tap recibe el mismo tráfico que si estuviera en línea, incluyendo todos los errores. Ver figura 15 para más detalles. Ni la fragmentación ni la regeneración introducen retrasos o cambian el contenido de la estructura de los paquetes de información.

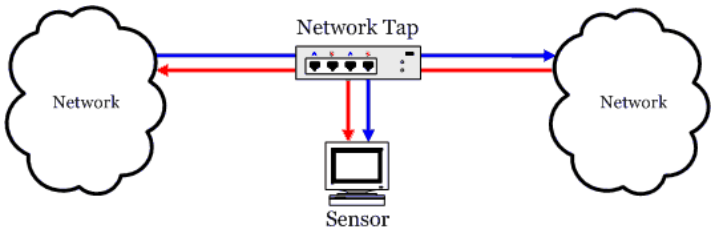

Figura 15: *Monitorización pasiva de red*

Por otra parte, un puerto *span* de un conmutador no ve todo el tráfico. Los paquetes de red dañados, paquetes de tamaño por debajo del mínimo, y errores de nivel 1 y 2 son normalmente descartados por el conmutador.

2. **Retrasos:** Los Taps dejan pasar los datos en modo *full-duplex* a la velocidad de la línea sin afectar al tráfico.

   Por el contrario, la arquitectura software de algunos conmutadores de bajo nivel introducen retrasos al copiar los paquetes para los puertos *span*. Peor aún, en muchos casos la información se envía a través de un puerto gigabit, introduciendo retrasos al convertir la señar de eléctrica a óptica.

   Además, el acceso al tráfico del conmutador está limitado por la capacidad del puerto *span*. Si el tráfico es excesivo, dicho puerto descartará paquetes, por lo que se perderá información. Por ejemplo, para poder ver el tráfico full-duplex de un enlace de 100 Mbps, el puerto *span* debe tener una capacidad de hasta 200 Mbps.

3. **Recursos:** Como los *Network Taps* son dispositivos pasivos, se pueden dejar permanentemente en línea sin afectar al tráfico.

   Por el contrario, los puertos *span* consumen recursos del conmutador, disminuyendo su rendimiento.

4.3. Ejemplos de implementación

Hay muchas formas de implementar análisis de tráfico de red con Taps. A continuación se describen tan sólo un par de ejemplos.

4.3.1. Sensor con dos interfaces de red

La figura 15 representa una forma de analizar tráfico, utilizando un sensor con dos interfaces de red, una para cada sentido del tráfico. Además de las interfaces, es necesario instalar algún tipo de software que permita combinar los datos de ambas interfaces físicas en una única intefaz lógica. Se puede utilizar por ejemplo el software *Sun Trunking* [13], o el controlador de red de Linux *bonding*. En este último caso primero hay que compilar el controlador *como módulo*, y luego combinar las interfaces de red físicas en una interfaz lógica (`bond0`). Por ejemplo, si deseamos vincular las interfaces físicas `eth1` y `eth2` a la interfaz lógica `bond0` con dirección IP 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)
```

No hace falta decir que el soporte ARP está deshabilitado debido a que no es necesario en un dispositivo de sólo recepción. Como `bond0` es una interfaz lógica, puede ser utilizada por `tcpdump`. La interfaz `eth0` puede ser utilizada para controlar remotamente el `sniffer`, o para enviar alertas a una consola central. Se puede leer más información sobre `bonding` en el fichero `Documentation/networking/bonding.txt` del código fuente de Linux.

4.3.2. Utilizando un *span-port* de un conmutador

Por otra parte, si tenemos un conmutador con puertos *span*, podemos probar la implementación de la figura 16, de Jeff Natham [15]. Describe cómo analizar tráfico de red utilizando un puerto *span* de 100 Mbps o 1000 Mbps.

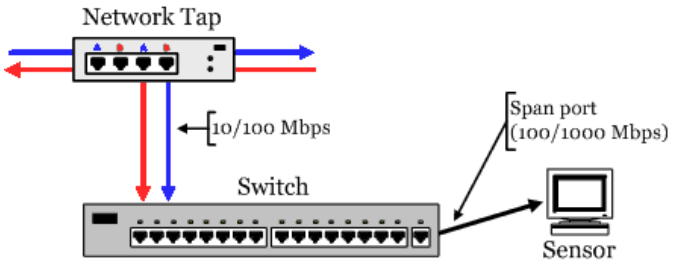

Figura 16: *Análisis con 'Network Tap' y puerto 'span' de un conmutador*

4.3.3. Balanceo de carga. Múltiples IDSs

Cuando se monitoriza tráfico de alta velocidad (Gigabit en fibra óptica o mejor) es recomendable utilizar múltiples sistemas IDS y balancear la carga entre ellos. La figura 17 indica cómo implementar este tipo de configuración [16]. Netoptics también ofrece una detallada guía de instalación [17] para uno de sus Gigabit Taps de fibra.

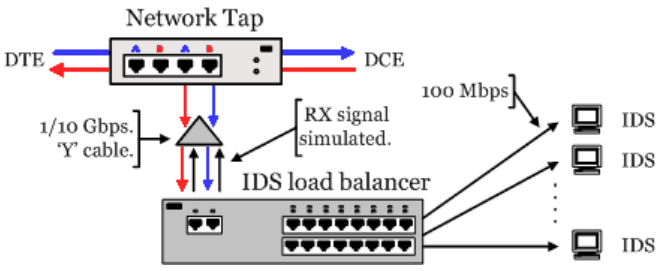

Figura 17: *Análisis de tráfico de alta velocidad*

5. Conclusiones

Los cables UTP de sólo recepción son baratos y una forma sencilla de monitorizar pequeñas redes caseras y de PYMES. Sin embargo, cuando las redes a examinar son mayores, como las redes corporativas que poseen grandes cantidades de ordenadores, es necesario contar con dispositivos profesionales que tengan facilidades de escalabilidad. Se deben utilizar Network Taps si se requieren dispositivos avanzados capaces de monitorizar conexiones de alta velocidad.

La necesidad de monitorizar y analizar tráfico de red ha aumentado y lo continuará haciendo. Esto se debe tanto a la necesidad de mejorar la seguridad como de conocer mejor nuestras propias infraestructuras IT. Cada situación requiere una solución diferente. Espero que este artículo haya descubierto al lector algunas alternativas que se adapten a su entorno.

Referencias

[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