2.3.3 使用网络分流器

大家都知道这句谚语：「有牛排可以吃的时候，为什么要选择鸡肉呢
（或者是美国南方的谚语，「有炸腊肠吃的时候，为什么要选择火腿呢?」）。
这种选择，也适用于使用网络分流器与集线器输出的对比上。

网络分流器是一个硬件设备，你可以将它放置在网络布线系统的两个
点之间，来捕获这两个端点之间的数据包。与集线器输出类似，在网络上
置一个硬件，就可以捕获你所需要的数据包。所不同的是，这次你并不是
用集线器，而是使用一个专门为了网络分析而设计的特殊硬件。

网络分流器又分为 2 种基本类型：聚合的和非聚合的。这两种分流器
是安置在两个设备之间，来嗅探所有流经的网络通信的。他们之间根本的
别在于：非聚合的网络分流器有 4 个端口，如图 2-7 所示，而聚合分流器
只有 3 个端口。

图 2-7　一款 Barracuda 的非聚合网络分流器

网络分流器通常还需要一个电源连接，但也有一些是带电池的，它们
需要插入电源插座就可以进行短暂的数据包嗅探。

1．聚合的网络分流器

聚合的网络分流器的使用方法是较简单的。它只有一个物理的流量监
口，来对双向通信进行嗅探。

为了使用聚合的网络分流器来捕获接入交换机的单台计算机的所有流
量，你只需要按照如下步骤进行操作。

（1）从交换机上拔下目标计算机的网线。

（2）将连接目标计算机网线的另一端插入到网络分流器的「in」端口中。

（3）将另一根网线的一端插入到网络分流器的「out」端口，并将另端插入到网络交换机。

（4）将最后一根网线的一端插入网络分流器的「Monitor」端口，并另一端插入到你作为嗅探器使用的电脑上。

聚合网络分流器的连接应该如图 2-8 所示的那样，一旦连好之后，你嗅探器就能够捕获到你接入网络分流器的所有网络流量。

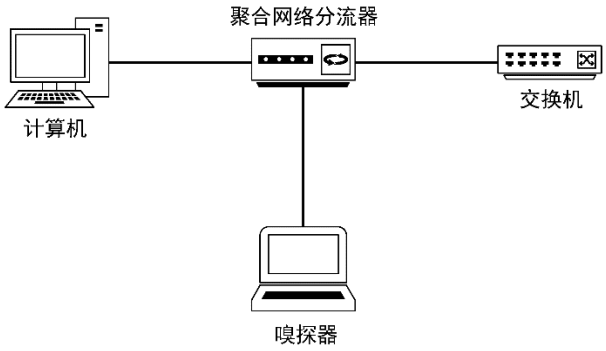

图 2-8　使用聚合的网络分流器来嗅探网络流量

2．非聚合的网络分流器

非聚合的网络分流器比起聚合的稍微复杂一些，但它在进行流量捕获有着更好的灵活性。与聚合网络分流器仅仅只有一个监听端口来嗅探双向信流量不同的是，非聚合的网络分流器有着两个监听端口。一个监听端口来嗅探流出方向的网络流量（从电脑连接到分流器的方向），另一个监听口用来嗅探流入方向的网络流量（从分流器端口到电脑的方向）。

为了捕获连接交换机的计算机的所有网络流量，你则需要按照如下步进行配置。

（1）从交换机上拔下计算机连接网线。

（2）将网线的一端插入计算机，另一端插入到网络分流器的「in」端口上。

（3）将另一根网线的一端插入到网络分流器的「out」端口，然后将一端插入到网络交换机上。

（4）将第三根网线插入到网络分流器的「Monitor A」端口，并将另端插入到你作为嗅探器使用电脑的一块网卡接口上。

（5）将最后一根网线插入到网络分流器的「Monitor B」端口，并将一端插入到你作为嗅探器使用电脑的第二块网卡接口上。

非聚合网络分流器的连接方式如图 2-9 所示。

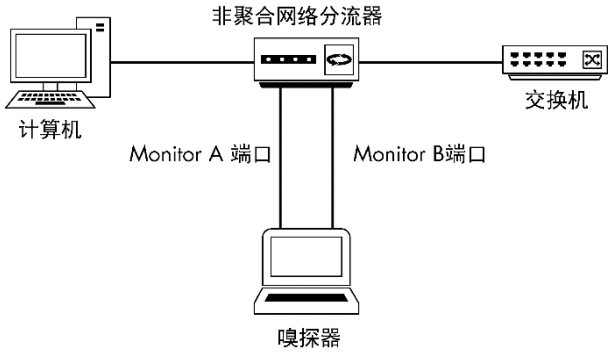

图 2-9　使用非聚合的网络分流器来嗅探网络流量

虽然以上的例子容易让你产生一种错觉，就好像你只能使用分流器监一台设备，但实际上你可以通过合理的规划，把分流器放置在合适的位置将其用来捕获多台设备的流量。例如，如果想在因特网上监听两个网络之的流量，你需要将集线器串联在所有设备相连的交换机和网络上层路由器间。这样的放置方式可以让你收集到所有你想要的流量。这种策略常常在全监控中用到。

3．选择一款网络分流器

网络分流器拥有两种不同的类型，那么哪种会更好一些呢？在大多数况下，聚合的网络分流器是首选，因为它们需要较少的网线，同时在嗅探计算机上也不需要两块网卡。然而，在你需要捕获高带宽的流量，或是只要关注一个方向上的流量时，非聚合的网络分流器会更加适用。

你可以购买到各种规格的网络分流器，从简单的大概 150 美元左右就买到的以太网分流器，到需要数万美元的企业级光纤分流器。我曾经使用 Net Optics 和 Barracuda 网络的网络分流器，觉得它们的产品都非常不错我敢肯定，市面上还有很多其他非常不错的选择。