HongKe 虹科

网络监控和数据包采集便携性的未来

VISIT www.hongwangle.com

“随身携带网络分路器TAP是分析网络问题的最佳方式之一。拥有便携式TAP是最好的和最快的方法，可直接进入您的网络，解析位置上的流量，并找出在危机时造成所有麻烦的数据包。”

现场网络监控

这个超级连接的世界及其日益复杂的IT环境为企业发展和创新提供了数十种巨大的可能性。

但是，所有这些都是有代价的，如果您查看一下安全漏洞，最新一波的勒索攻击浪潮刚刚暴露出来。物联网暴露了网络攻击渗透网络并造成重大财务，业务和声誉损失的新方法。

如今，您不能百分百确定自己的公司不会在某个时候受到某种勒索软件攻击。但这并不意味着您无法采取所有必要的预防措施，这样您有足够的能力应对此类攻击。

网络的安全性必须从IT基础结构内部开始，因为网络问题和安全性问题可能会发生，尤其是在您最意想不到的时候。当您正处于这样的网络危机之中时，甚至更好的是，在危机发生之前，您需要一个能够部署快速，解决迅速且功能强大的网络分析仪。换句话说，您需要快速全面地了解网络上正在发生的事情。

为了对网络上的问题进行正确的评估，查看您可以获得的所有信息非常重要。从那里可以对信息进行过滤并深入到问题的根本原因。实现此目标的最佳方法之一是使用网络分路器TAP。如果没有100%访问网络上发生的情况，即使是最好的网络工程师也无法正确评估情况。

随身携带网络分路器TAP是分析网络问题的最佳方式之一。拥有便携式TAP是最好的和最快的方法，可直接进入您的网络，解析位置上的流量，并找出在危机时造成所有麻烦的数据包。

但是，并非所有便携式分路器TAP都像听起来那样出色。其中一些功能强大但处理起来很复杂。它们中的一些易于部署，但功能不足以处理整个交通。因此，具有强大功能的便携式分路器TAP就是最好的工具，它足以承担100%的流量，而且现场部署简单、快捷。

目前，无论在现场还是市场上，我们看到了不同版本的便携式分路器TAP。在网络监控领域中，对便携的定义有所不同。 您如何在这种充满选择和可能性的迷宫中导航呢？市场上最新添加了哪些产品，我们未来的发展方向是什么？

在接下来的几页中，我们将为您概述市场上最常见的选择以及它们的优缺点。

便携式全双工分路器

一些制造商推出了其全双工TAP的基本版本，并将其作为便携式型号进行销售。但是，它们足够小，仅可满足一条链路的需求。基本上，它们是机架安装型的较小版本，仍然包含机架安装式螺丝夹。

作为全双工分路器，它确实以全线速捕获流量，而没有任何数据包丢失或定时延迟。所以性能是有的，但是对于IT工程师来说，在现场随身携带这样的“便携式” 分路器仍然很困难，因为需要额外的硬件。（见图1）

全双工分路器，或分路分路器从两个网络端口捕获流量并将其复制到两个“输出”或监视端口。这就是使现场事情复杂化的原因。除了全双工分路器本身，您还需要有一台包含双网卡（NIC）的便携式PC。除此之外，托管监视应用程序的PC还必须执行接口绑定或链接聚合，以将两个接口“视为”单一的流量流。

这意味着双倍资源、双倍成本和双倍的时间来开始您的网络分析。让我们接受这一点 – 您不能在野外随身携带台式机，而且笔记本电脑中也没有双网卡。（有多少公司向其工作人员提供双NIC高性能笔记本电脑？）

如您所见，就网络分路器而言，纸上的便携性和实践中的便携性是两个截然不同的方面。

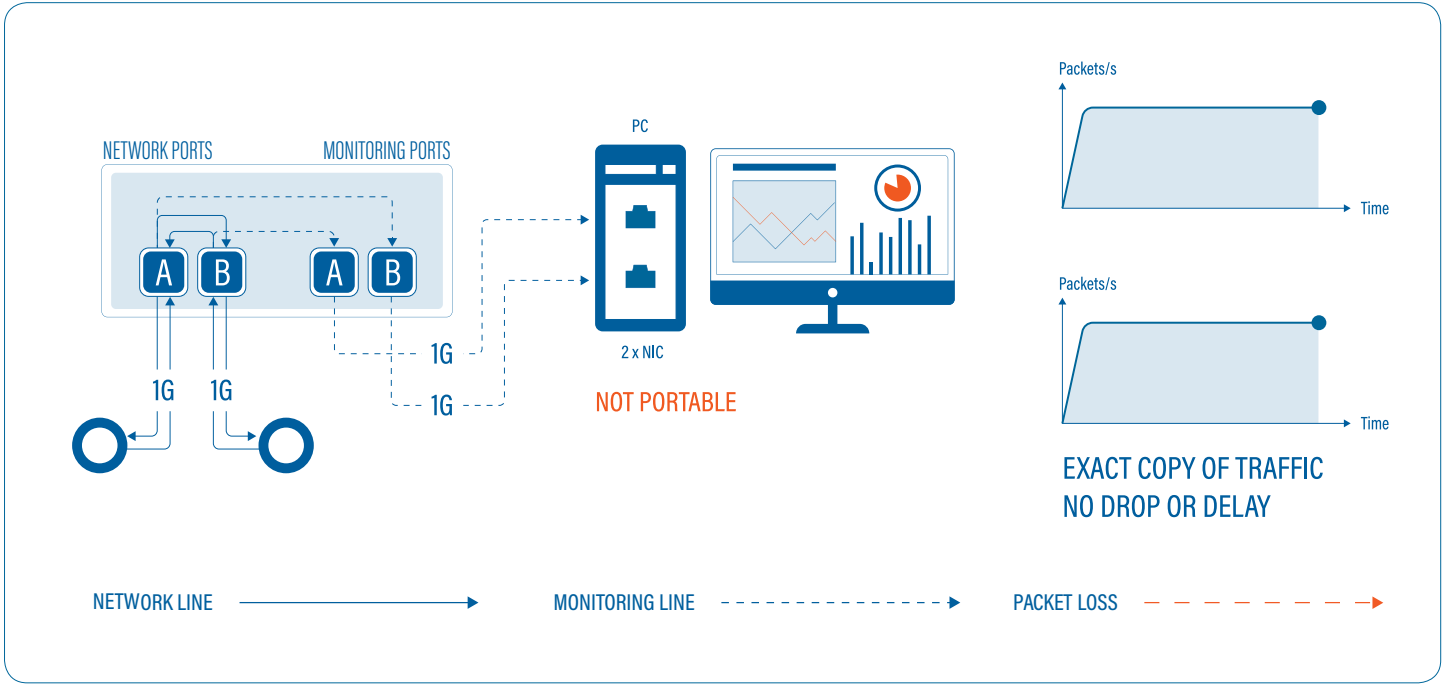
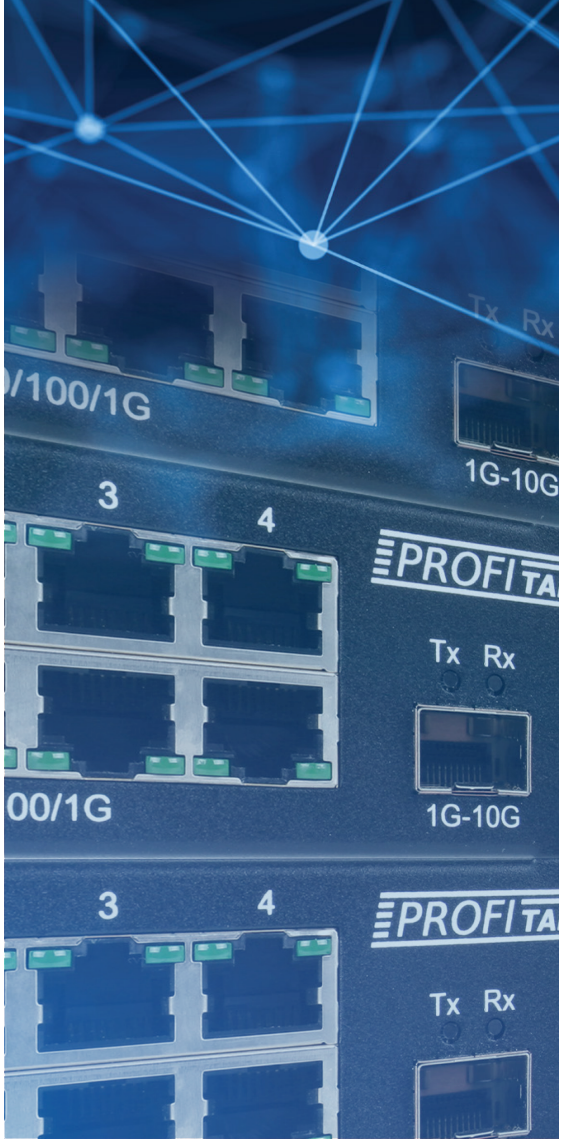


图 1: 全双工分路器的示意图



便携式聚合分路器

分路器制造商解决全双工分路器需要额外资源问题的另一种方式是引入聚合分路器。顾名思义，聚合分路器将两个输入的流量流合并为一个输出的流量流。因此，存在接收两个网络端口聚合流量的单个监视端口。

这解决了分析PC中对双NIC的需求。实际上，它完全不需要配备便携式PC，使您的笔记本电脑可以轻松连接到分路器。便携式实现了，但以牺牲性能为代价。

如果分路器中的输入和输出端口具有相同的数据速率，那么这本身可能会成为问题。我们都知道，当今的网络干线至少是千兆速率（1Gbps）。因此，要对任何网络干线进行故障排除，必须使用千兆端口设置分路器。但是，当输出（或监控端口）也是千兆位端口时，则不可能在1Gbps输出上完全传输2Gbps的组合流量流。这意味着流量捕获是不一致。 （见图2）

聚合分路器使用内部缓冲区来聚合流量并缓存传入的数据包，以跟上输出端口的速度。但是，这取决于缓冲区的大小，在开始丢弃传入的数据包之前，它可以维持它们多长时间。

一旦网络接口利用率超过50%以上，并且缓冲区已满，您的数据包将开始从网桥上丢失。如果两个输入网络端口都以最大容量限制流量，则可能会丢失多达50%的总流量。某些聚合TAP拥有更多的内存来吸收数据突发，但这是以对数据包时序产生重大影响为代价的，这不适用于分析实时协议。

克服此瓶颈的最佳方法是将聚合的流量传输到更高的数据速率输出。对于分路器制造商来说，在便携式分路器中使用10GE网卡作为输出是不可行的。此外，笔记本电脑不具有10GE NIC，并且可能一段时间不会使用。重点是将便携性和性能打包到一个小设备中。

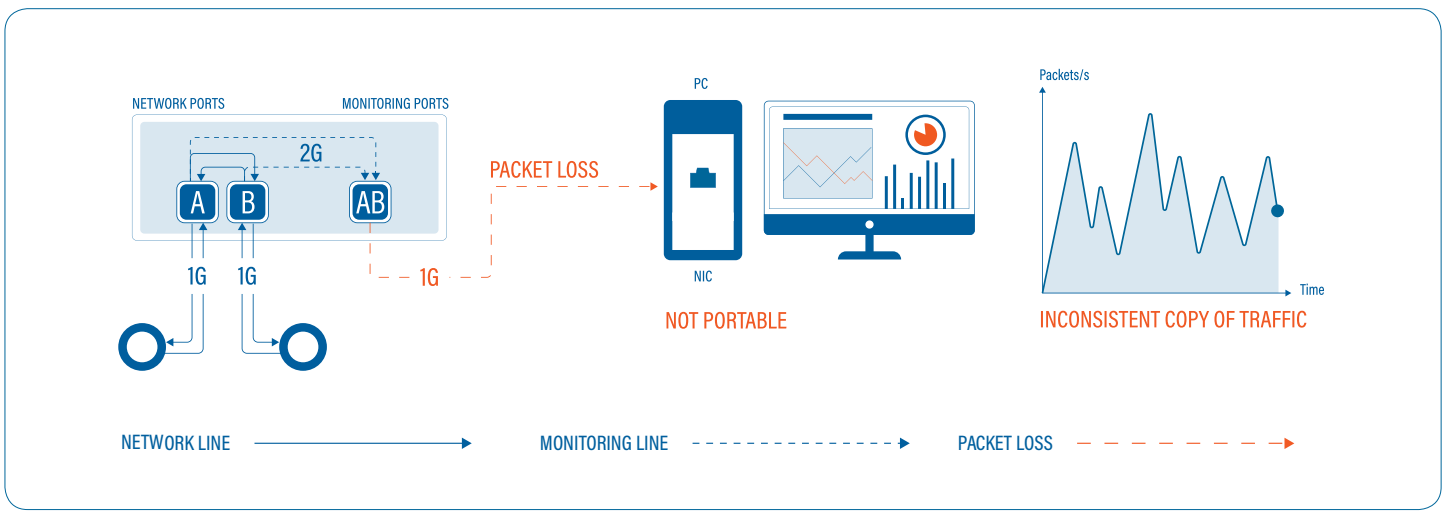


图2: 聚合分路器示意图

“ProfiShark 1G是专门为处理各种故障排除而设计的，可在任何现场位置使用，袖珍大小且功率强大。它用作聚合TAP，但不会导致数据包丢失或时间延迟的瓶颈。借助两个千兆网络端口，它将两个业务流无缝组合到一个监控端口中。”

PROFISHARK真正的便携性

因此，有没有可以为您提供完全便携性和必要性能的分路器呢？ProfiShark系列是便携式网络分接领域中的最新发展之一。

在ProfiShark系列中，我们将重点介绍ProfiShark 1G，以便与前面提到的网络分路器进行公平比较。

ProfiShark 1G是专门为处理各种故障排除而设计的，可在任何现场位置使用，袖珍大小且功率强大。它用作聚合TAP，但不会导致数据包丢失或时间延迟的瓶颈。借助两个千兆网络端口，它将两个业务流无缝组合到一个监控端口中。

它不使用千兆网卡作为监视端口。而是利用USB 3.0的功能，该功能可以高达5 Gbps的速度传输数据。 因此，它可以通过USB 3.0链路轻松传输2 Gbps的聚合流量（从端口A和B分别输出1G）。这意味着缓冲存储器不需要丢弃任何数据包，也不必存储足够长的数据包来影响其时序。 （见图3）

由于它连接到笔记本电脑的USB端口，因此具有独特的即插即用功能，而无需依赖外部电源。

ProfiShark 1G捕获数据包并将其直接传输到任何主机计算机的磁盘。当每个数据包进入分路器时，将在硬件级别使用纳秒级时间戳实时捕获所有数据包。这允许以纳秒分辨率对捕获的流量进行实时协议分析。

如今的分路器不仅可以为您提供对便携式包装中的网络线路的完全访问权限，而且还可以用作长期捕获解决方案并可以远程访问。

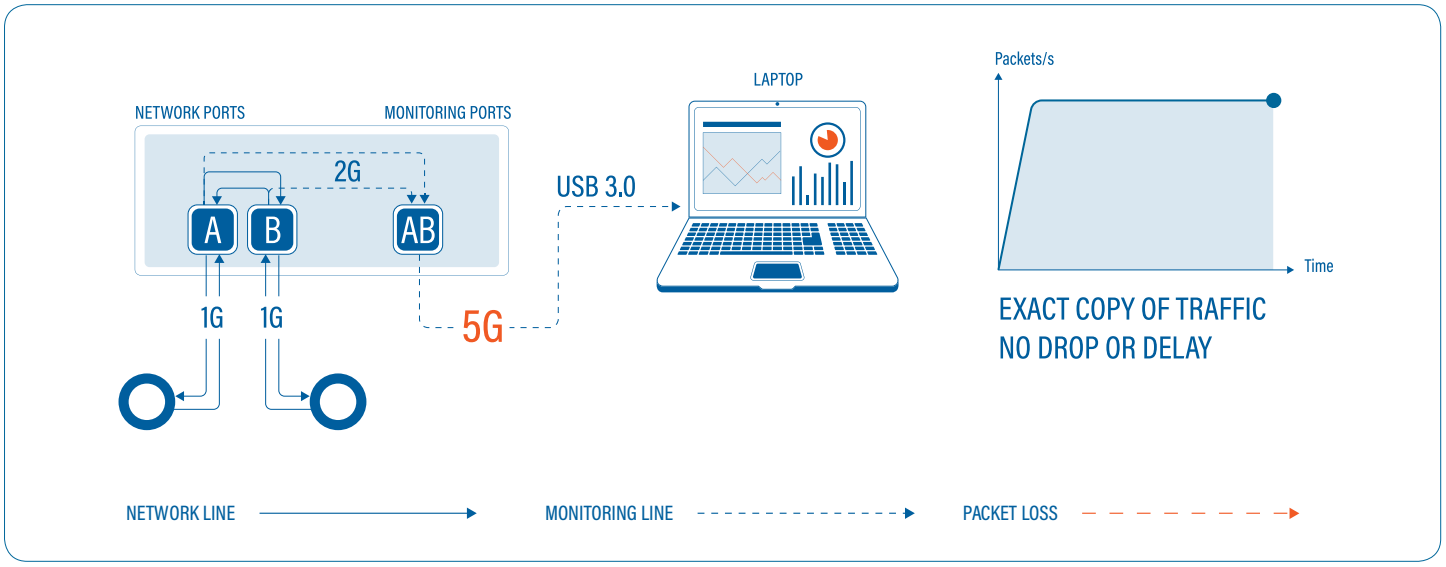


图 3: ProfiShark 1G分路器示意图

“长期捕获功能与具有为您的特定需求量身定制的NAS相结合，使其成为捕获间歇性问题的理想工具，同时仍是当今市场上最便携的解决方案。”

使用PROFISHARK 1G进行长期捕获

网络工程师通常会在故障排除情况下发现自己所寻找的问题只是偶尔发生，从而使其无法重现。捕获间歇性问题可能非常困难，并且会占用捕获设备的大量空间和时间。如果您仅可以开始捕获，让其运行直到问题发生并在以后的某个时间点分析捕获文件，这不是很容易吗？

当然，知道您要查找的内容仍然很重要，因此您不必挖掘千兆字节甚至TB级的信息即可找到所需的数据包。ProfiShark借助灵巧的硬件过滤和数据包切片功能帮助您。

长期捕获功能与具有为您的特定需求量身定制的NAS相结合，使其成为捕获间歇性问题的理想工具，同时仍是当今市场上最便携的解决方案。

HongKe 虹科

广州虹科电子科技有限公司

需要详细信息？请通过sales@hkaco.com联系我们

电话: 400-999-3848

广州 | 北京 | 上海 | 深圳 | 西安 | 武汉 | 成都 | 沈阳 | 香港 | 台湾 | 美国

产品信息

技术案例