网络安全:巧用嗅探器保障网络稳定运行Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/571/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_571815.htm 对于网络、系统管理或安全技术人员来说，在对网络进行管理和维护的过程中，总会遇到这样或那样的问题。例如，网络传输性能为什么突然降低？为什么网页打不开，但QQ却能上线？为什么某些主机突然掉线？诸如此类的网络问题一个又一个地不断出现，都需要我们快速有效地去解决，以便能够尽量减少由于网络问题对企业正常业务造成的影响。因此，我们就需要一引起工具来帮助我们快速有效地找出造成上述这些问题的原因。 网络嗅探器就是这样的一种网络工具，通过对局域网所有的网络数据包，或者对进出某台工作站的数据包进行分析，就可以迅速地找到各种网络问题的原因所在，因而也就深受广大网络管理员和安全技术人员的喜爱。 可是，我们也应该知道交换机是通过MAC地址表来决定将数据包转发到哪个端口的。原则上来讲，简单通过物理方式将网络嗅探器接入到交换机端口，然后将嗅探器的网络接口卡设为混杂模式，依然只能捕捉到进出网络嗅探器本身的数据包。这也就是说，在交换机构建的网络环境中，网络嗅探器不使用特殊的方式是不能分析其它主机或整个局域网中的数据包的。但是，现在的企业都是通过交换机来构建局域网，那么，如果我们要想在这样的网络环境中使用网络嗅探器来解决网络问题，就必需考虑如何将网络嗅探器接入到目标位置，才能让网络嗅探器捕捉到网络中某台主机或整个网段的网络流量。 就目前来说，对于在交换机构建的网络环境中使用网络嗅探器，可

以通过利用可网管交换机的端口汇聚功能、通过接入集成器或Cable TAP接线盒及选择具有特殊功能的网络嗅探软件这3种方法来进行。这3种可行的方式分别针对不同的交换机应用环境来使用的，本文下面就针对目前主流的几种交换机网络环境，来详细说明这3种接入方式的具体应用。 通过可网管交换机端口汇聚功能来达到目的 现在一些可网管式交换机，一般都有一种叫做端口汇聚（port spanning）的功能，并且带有一个可以用来实现这种功能的端口。使用交换机的端口镜像功能时，就允许我们将交换机中其它端口上的流量镜像到这个特殊的端口当中。这样，只要将网络嗅探器连接到这个端口上，然后将嗅探器的网络接口卡设为混杂模式，就可以嗅探到所有由交换转发的数据包。 要想使用交换机的端口汇聚功能，在使用前必需对交换机进行相应的设置。设置的方法得根据交换机可以使用的配置功能来进行，有些交换机可以通过终端方式来进行，也可以通过WEB方式更加直观地设置交换机的端口汇聚功能，还可以通过远程登录的方式进行设置。为了保障交换机的安全，最好使用本地登录方式的终端管理模式和本地WEB管理模式。图1.1就是通过端口汇聚功能接入网络嗅探器的拓扑图。图1.1 通过端口汇聚方式接入网络嗅探器的拓扑图 现在，在一些中小型的企业当中，由于网络规模不大，或者为了节省IT成本，只使用了一些非网管的交换机来构建局域网。对于非网管型的交换机，我们就不可能再使用端口汇聚功能来接入网络嗅探器了。那么，对于这种交换机构建的网络环境，我们又该使用什么样的方法来达到嗅探网络中的所有网流数量，或者只嗅探进出某台工作站之中的网络流量的目的呢？ 就目前来说，在这样的交换机网

络环境中可以使用下面所示的两种方法来实现：第一种方法就是通过在交换机上再接入一个小型集线器（HUB），然后将嗅探器和被嗅探的所有主机都连接到这个集线器中。这样，就使被嗅探的网络变成了共享式的以太网，在这个重新构建的共享式局域网中的所有数据包，将会以广播的方式发送到集线器的所有端口。如此一来，只需要将网络嗅探器的以太网网卡置于混杂模式，就可以嗅探到这个共享式局域网中传输的所有数据包。 但是，使用这种方式有它一定的局限性的。一方面，将一个关键的网络段连接到集线器上，由于所有的工作站都是共享集线器的带宽的，接入的工作站过多就会影响到它们的网络性能。另一方面，如果在构建局域网时没有考虑到网络嗅探器的使用，也就不可能在一开始就连入了集线器。因而在局域网运行过程中再将集线器接入到交换机上时，就不得不中断网络，以及将它从交换机中退出时，也会中断一次网络。因此，这种接入网络嗅探器的方式只有当出现了某种严重的网络问题，需要用网络嗅探器来分析解决时才能使用。图2.1就是通过集线器连入网络嗅探器的拓扑图。图2.1 通过集线器的方式连入网络嗅探器的拓扑图 第二种方法就是通过在交换机上接入一个Cable TAP接线盒，然后将网络嗅探 器和所有需要被管理的工作站或服务器连接到Cable TAP接线盒上，由于它也是一种共享式网络连接设备，因而也就可以嗅探到使用它构建的整个局域网中传输的所有数据包了。 