交换机端口监控-SPAN

　　在交换以太网的环境下，一般两台工作站之间的通讯是不会被第三者侦听到的。在某些情况下，我们可能会需要进行这样的侦听，如：协议分析、流量分析、入侵检测。为此我们可以设置Cisco交换机的SPAN (Switched Port Analyzer交换端口分析器)特性, 或早期的“端口镜像”、“监控端口”功能。

　　侦听的对象可以是一个或多个交换机端口，或者整个VLAN。假如要侦听的端口(“源端口”)或VLAN和连接监控工作站的端口(“目标端口”)在同一台交换机上，我们只需配置SPAN; 假如不在同一台交换机上，需要配置RSPAN (Remote SPAN)。不同的交换机对SPAN有不同的限制，如2900XL交换机中源端口和目标端口必须在同一VLAN、某些交换机不支持RSPAN等等，详见设备文档。

　　在配置SPAN的时候，我们需要提供的参数是源端口或VLAN号以及目标端口。

　　4000/6000 CatOS 交换机:

　　set span 6/17 6/19 //SPAN:源端口为6/17 目标端口为6/19

　　2950/3550/4000IOS/6000IOS 交换机：

　　monitor session 1 local //SPAN

　　monitor session 1 source interface fastethernet 0/17 both //源端口，也可以是某个VLAN

　　monitor session 1 destination interface fastethernet 0/19 //目标端口

　　2900/3500XL 交换机：

　　interface fastethernet 0/19 //目标端口

　　port monitor fastethernet 0/17 //源端口

　　1900 交换机: (或使用菜单 [M] Monitoring)

　　monitor-port monitored 0/17 //源端口(0/17和0/18端口)

　　monitor-port monitored 0/18

　　monitor-port port 0/19 //目标端口

　　monitor-port //开始监控

　　在配置RSPAN的时候，我们首先要定义一个类型为RSPAN的VLAN。在普通VLAN上假如源主机和目标主机都在同一台交换机上，则它们之间的单播通讯不需要通过TRUNK传递到别的交换机，而RSPAN VLAN需要在TRUNK上转发这样的通讯，以保证监控机能够侦听到。在源交换机上，需设置使被侦听的端口或VLAN把流量转发到RSPAN VLAN上(假如是运行IOS的交换机，需要另外设置一个端口作为反射端口); 在目标交换机上，需设置把RSPAN VLAN中的信息转发到连接监控主机的目标端口。

　　IOS交换机,如3550:

　　3550(config)#vlan 900 //建立RSPAN VLAN

　　3550(config-vlan)#remote-span

　　monitor session 1 remote //源交换机

　　monitor session 1 source interface fastethernet 0/17 both //源端口

　　monitor session 1 destination remote vlan 900 reflector-port fastethernet 0/20 //目标RSPAN VLAN，反射端口

　　monitor session 2 remote //目标交换机

　　monitor session 2 source remote vlan 900 //RSPAN VLAN

　　monitor session 2 destination interface fastethernet 0/19 //目标端口

　　CatOS 交换机，如6500:

　　set vlan 900 rspan //建立RSPAN VLAN

　　set rspan source 4/1-2 900 //源交换机

　　set rspan destination 4/19 900 //目标交换机

　　最近一次配置完RSPAN之后，有用户反映：部分网段出现严重丢包现象。仔细检查，发现部分交换机的上联端口负载很重。再分析，原来在两台中心交换机上启用了一个RSPAN进程，RSPAN VLAN上的流量很大，达300M。由于VTP 域中没有启用PRuning 功能，这个RSPAN VLAN的流量出现在所有的TRUNK上，造成了阻塞。把RSPAN VLAN从这些TRUNK上修剪掉之后，网络恢复了正常。

　　SPAN功能的出现，使保护交换机不被非法控制变得更为重要。因为假如黑客控制了一台主机和部分交换机，他将能够使用SPAN/RSPAN和Sniffer窃听任何在网络上传递的信息。