镜像技术原理及配置

一、镜像技术的概念

1、在网络维护的过程中会遇到需要对数据进行获取和分析的情况，如：怀疑有攻击数据；此时需要在不影响数据转发的情况下，对数据进行获取和分析

2、镜像技术可以在不影响数据正常处理流程的情况下，将镜像端口的数据复制一份到观察端口，用户利用数据监控设备来分析复制到观察端口的数据，进行网络监控和故障排除

二、数据采集的作用

1、业务实时监控：

大型网络或数据中心一般会在汇聚点设置监控系统实时监测网络数据流量信息，防范和防止业务的异常

2、故障处理分析：

一些疑难杂症的故障需通过采集实际的报文信息来找到更加明显的线索

3、网络流量优化：

当网络系统发展到一定规模，对数据流量地精细化控制变的尤为重要，只有实际采集现网的真实数据流量，通过专业的流量分析系统定位出网络的各种问题，并为此提出优化解决方案

三、数据采集的方式

1、分光器物理采集：

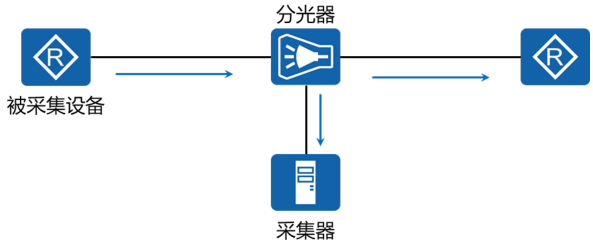
1.1、利用物理器件【分光器】插入连接的链路中，复制出正常的数据流至采集器

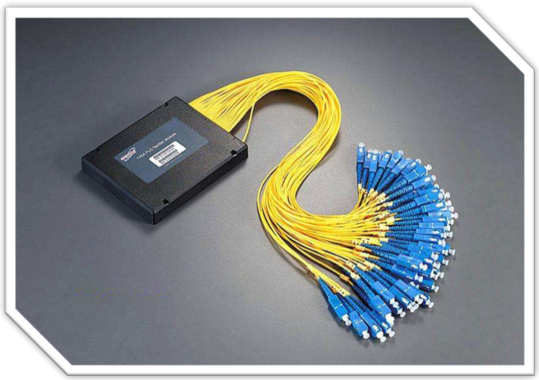
1.2、分光器采集的优缺点：

a、采集的数据完整可靠，只在中间链路上操作，完全不影响被采集设备的性能，也不占用链路带宽

b、缺点为每次采集要做物理动作切入，相对繁琐且有风险

c、适合网络业务出入口大型设备的数据流采集，常用于连接IDS设备网络环境





2、NMS【Network Management System | 网络管理系统】集中采集：

2.1、利用通用标准协议SNMP【简单网络管理协议】传送标准的MIB数据，采集整网的配置信息和设备端口数据流信息

2.2、NMS采集的优缺点：

a、优点是可以采集整网设备节点的信息

b、缺点是针对接口的数据流信息采集不够精细和完整，大部分是统计信息

c、适合网管中心查看设备的参数和性能以及业务信息统计

注、SNMP的简要讲解

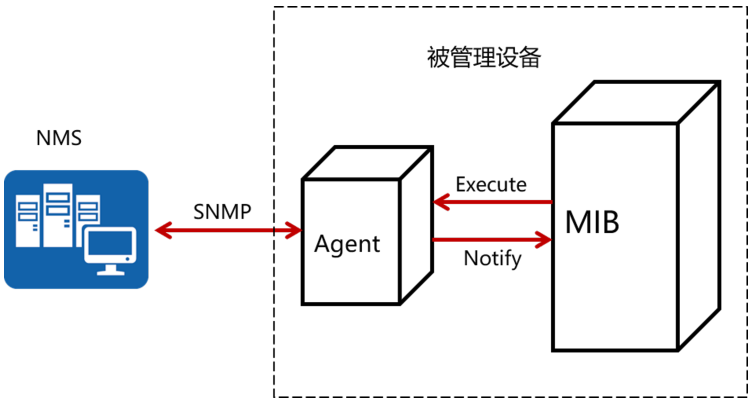
1、SNMP用来在网络管理系统【NMS】和被管理设备【路由器、交换机、防火墙等】之间传输管理信息

2、SNMP的架构包括：NMS【网络管理系统】、Agent【代理】、MIB【管理信息库】

2.1、NMS是运行在网管主机上的网络管理软件；网络管理员通过操作NMS，向被管理设备发出请求，从而可以监控和配置网络设备

2.2、Agent是运行在被管理设备上的代理进程；被管理设备在接收到NMS发出的请求后，由Agent作出响应操作；Agent的主要功能包括：收集设备状态信息、实现NMS对设备的远程操作、向NMS发送告警消息

2.3、管理信息库MIB【Management Information Base】是一个虚拟的数据库，是在被管理设备端维护的设备状态信息集；Agent通过查找MIB来收集设备状态信息



3、SNMP的版本

SNMP共分为3个版本：

版本	描述
SNMPv1	实现方便，安全性弱
SNMPv2c	具有一定的安全性，现在应用最为广泛
SNMPv3	定义了一种管理框架，为用户提供了安全的访问机制

4、SNMP的配置

详细配置见HCIA-Datacom实验手册

3、镜像技术复制采集：

3.1、将镜像端口【源端口】的数据复制一份到观察端口【目的端口】

3.2、可获取完整数据，用于分析网络状况

3.2、镜像技术的优点：

a、不影响原有网络，快捷方便

b、采集的是实时数据流，真实可靠

4、镜像技术的特点：

4.1、镜像技术支持将多端口的流量镜像到同一个观察端口，配置时没有数量限制，但需要考虑观察端口实际的流量是否超过其转发能力，即实际流量是否超过此观察端口的最大带宽

4.2、若在主接口配置镜像技术，子接口的流量也将被镜像到观察端口

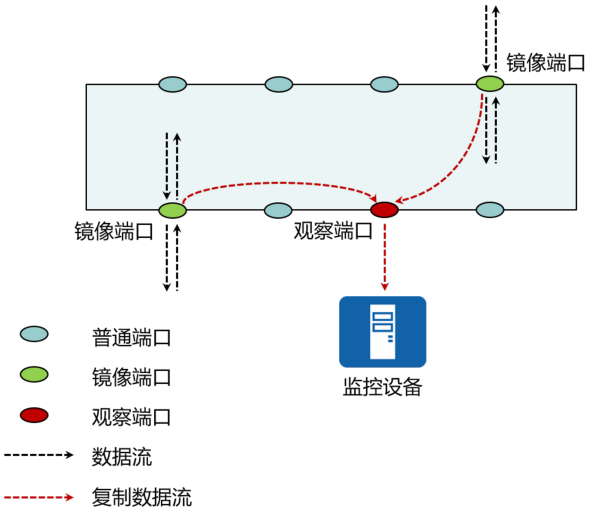
5、镜像技术端口角色

5.1、镜像端口：

镜像端口是被监控的端口，从镜像端口流经的所有数据或匹配流分类规则的数据将被复制到观察端口

5.2、观察端口：

观察端口是连接监控设备的端口，用于输出从镜像端口复制过来的数据



四、镜像技术的配置

详细配置见实验手册