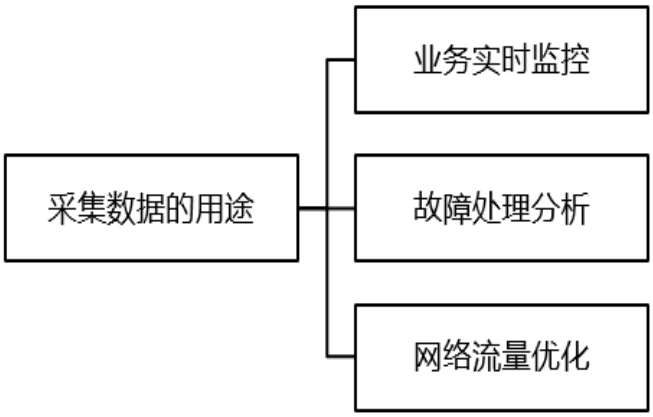
镜像技术原理与配置

前言

- 在网络维护的过程中会遇到需要对报文进行获取和分析的情况，比如怀疑有攻击报文，此时需要在不影响报文转发的情况下，对报文进行获取和分析。
- 镜像技术可以在不影响报文正常处理流程的情况下，将镜像端口的报文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报文，进行网络监控和故障排除。

数据采集的作用

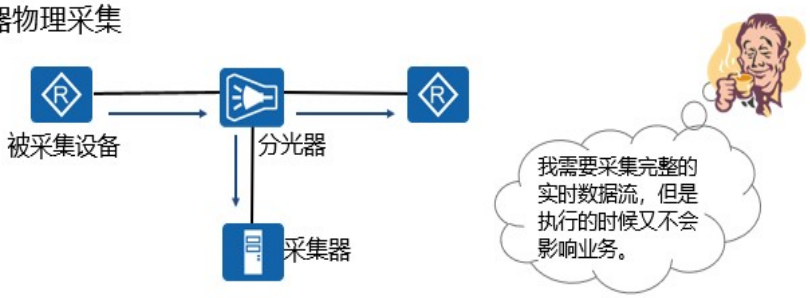


- 业务实时监控：
- 大型网络或数据中心一般会在汇聚点设置监控系统实时监测网络数据流量信息，防范和防止业务的异常。

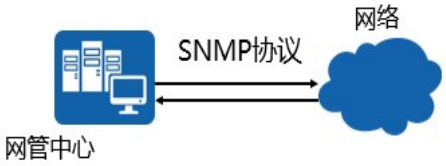
- 故障处理分析：
- 一些疑难杂症的故障需通过采集实际的报文信息来找到更加明显的线索。
- 网络流量优化：
- 当网络系统发展到一定规模，对数据流量地精细化控制变的尤为重要。只有实际采集现网的真实数据流量，通过专业的流量分析系统定位出网络的各种问题，并为此提出优化解决方案。

数据采集的方法

- 分光器物理采集



- NMS集中采集



- 分光器物理采集：
- 利用物理器件分光器插入连接的链路当中，复制出正常的数量流到采集器上面。
- 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。
- 缺点是每次采集要做物理动作切入，相对繁琐且有风险。
- 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 设备的网络环境。
- NMS 集中采集：
- 利用通用标准协议 SNMP 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。

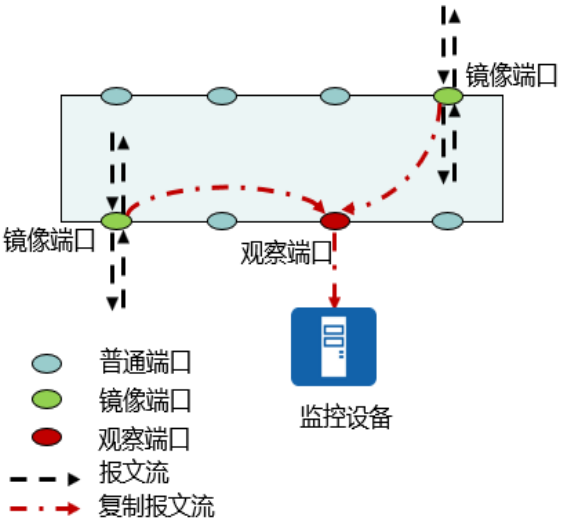
- 优点是可以采集整网设备节点信息。
- 缺点是针对接口的数据流信息采集不够精细和完整，大部分是统计信息。
- 适合网管中心查看设备的参数和性能以及业务信息统计。

镜像概述

- 镜像定义
  - 将镜像端口（源端口）的报文复制一份到观察端口（目的端口）。
- 镜像作用
  - 获取完整报文用于分析网络状况。
- 镜像优点
  - 不影响原有网络，快捷方便。
  - 采集的是实时数据流，真实可靠。

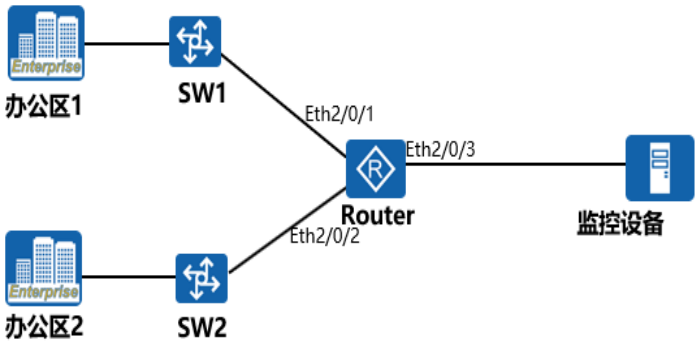
- 镜像的特点：
- 在网络维护的过程中会遇到需要对报文进行获取和分析的情况，比如怀疑有攻击报文，此时需要在不影响报文转发的情况下，对报文进行获取和分析。
- 镜像可以在不影响报文正常处理流程的情况下，将镜像端口的报文复制一份到观察端口，用户利用监控设备来分析复制到观察端口的报文，进行网络监控和故障排除。
- 镜像支持将多端口的流量镜像到同一个观察端口，配置时没有数量限制，但是需要考虑观察端口实际的流量是否超过其转发能力，即实际流量是否超过此观察端口的最大带宽。
- 如果在主接口做端口镜像，会将子接口流量也镜像到观察端口。

镜像的角色



- 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报文或匹配流分类规则的报文将被复制到观察端口。
- 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报文。

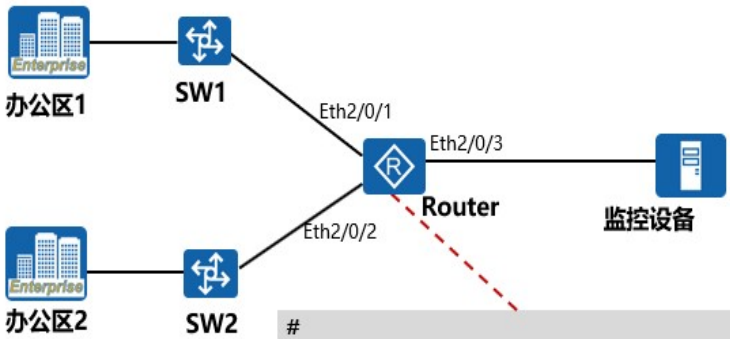
本地端口镜像配置需求



- 某企业中，办公区1和办公区2用户分别通过接口Eth2/0/1、Eth2/0/2接入Router。一台监控设备接在Router的接口Eth2/0/3上，用于数据分析监控。为保证企业的信息安全，用户希望通过监控设备对办公区1和办公区2发送的所有报文进行监控。

- 配置思路：
- 在 Router 上将接口 Eth2/0/3 配置为本地观察端口。
- 在 Router 上将接口 Eth2/0/1 和 Eth2/0/2 配置为镜像端口，实现对接口报文进行监控。

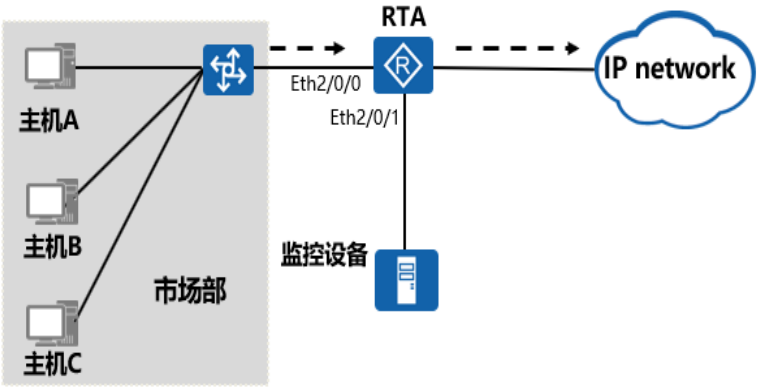
本地端口镜像配置实现




```
#
 observe-port interface Ethernet2/0/3
#
interface Ethernet2/0/1
 mirror to observe-port inbound
#
interface Ethernet2/0/2
 mirror to observe-port inbound
```

- 配置命令：
- #
- observe-port interface Ethernet2/0/3 //将 E2/0/3 接口配置为观察端口。
- #
- interface Ethernet2/0/1
- mirror to observe-port inbound //将 E2/0/1 接口配置为镜像端口，镜像所有入方向报文。
- #
- interface Ethernet2/0/2
- mirror to observe-port inbound //将 E2/0/2 接口配置为镜像端口，镜像所有入方向报文。

流镜像配置需求



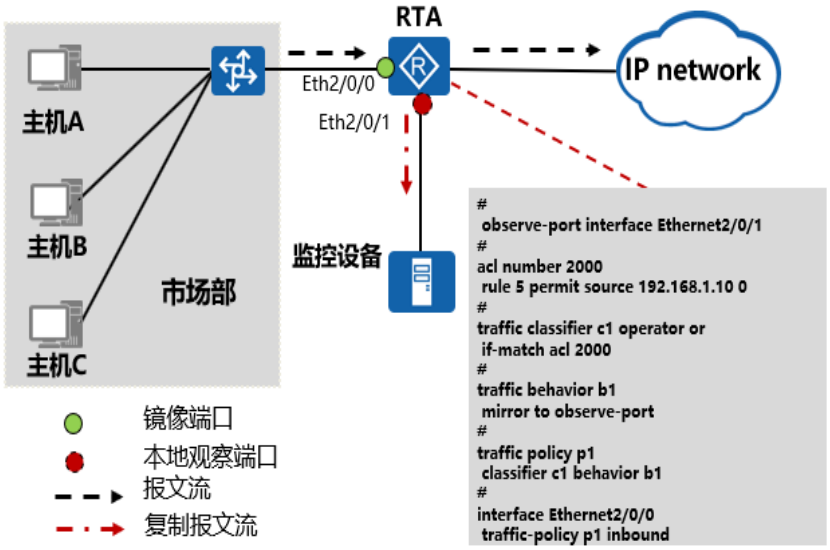
某企业中，市场部用户通过接口Eth2/0/0接入路由器RTA。一台监控设备接在RTA的接口Eth2/0/1上，用于数据分析监控。用户希望监控市场部IP地址为192.168.1.10的主机发出的所有报文。

- 流镜像：
- 将镜像端口上特定业务流的报文传送到监控设备进行分析和监控。在流镜像中，镜像端口应用了特定的流策略。如果从镜像端口流经的报文匹配流策略，则将被复制并传送到监控

设备。

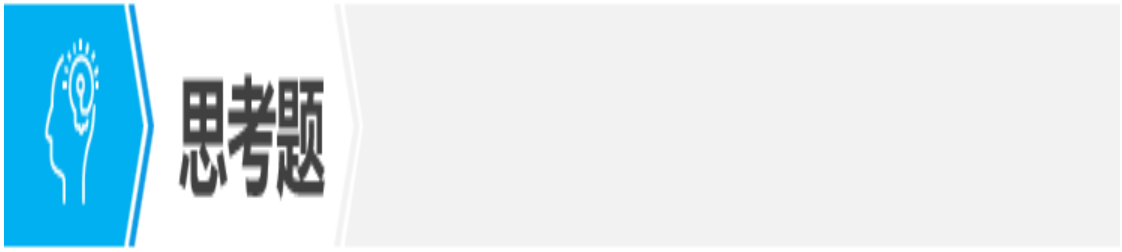
- 配置思路：
- 将接口 Eth2/0/1 配置为本地观察端口。
- 配置流镜像策略，并在接口 Eth2/0/0 入方向上应用流策略，将匹配源 IP 地址为 192.168.1.10 的报文复制到本地观察端口。

流镜像配置实现



- 配置命令：
- observe-port interface Ethernet2/0/1 //将端口 E2/0/1 定义为观察端口。
- #
- acl number 2000 //用 ACL 匹配 IP 为 192.168.1.10 主机。
- rule 5 permit source 192.168.1.10 0
- #
- traffic classifier c1 operator or
- if-match acl 2000
- #

- traffic behavior b1
- mirror to observe-port
- #
- traffic policy p1//定义流策略，将 ACL 匹配的流量镜像到观察端口。
- classifier c1 behavior b1
- #
- interface Ethernet2/0/0
- traffic-policy p1 inbound //在镜像端口 E2/0/0 入方向应用流策略。



- 答案：镜像的角色包括：镜像端口，观察端口。
- 答案：流镜像采集的是镜像端口上的特定业务流，端口镜像采集的是整个端口的业务流。
-