组合九（网关放置）

2020年3月15日 11:23

组合九：
理论：Netstream工作原理；交换机、路由器分别有哪些表项，如果不存在相应表项，数据如何处理 ；
项目：园区网关放置

Netstream的工作原理

传统流量分析工具的缺陷：

表1 传统的流量统计的实现方法和局限性

名称	实现方法	局限性
基于IP报文计数	在路由表中存放计数器索引，对通过设备的字节和包分别计数。	统计的信息简单，无法针对多种信息进行统计。
使用ACL	通过ACL精确的匹配流，匹配后进行计数。	要求ACL的容量很大，对于ACL规则以外的流没有办法统计。
SNMP协议	使用网管协议，能够实现一些简单的统计功能，比如接口计数、IP报文计数、ACL匹配计数等。	功能不强。要不断的通过轮询向网管查询，浪费CPU和网络资源。
端口镜像	通过端口镜像，把流量复制一份，发送至专用的服务器进行统计分析。	成本高，需要购买专用的服务器进行统计，同时消耗设备的一个接口，对于无法镜像的端口无能为力。
物理层复制	在物理层通过分光器或者其他设备复制流量，发送至专用的服务器进行统计。	成本高，需要购买专用的服务器进行统计，同时还需要购买专用的硬件设备。

计费：
NetStream可以统计包括IP地址、包数、字节数、时间、 ToS和应用类型等流量信息，实现灵活的计费
网络监控：
通过在连接Internet的接口部署NetStream，可以对网络出口进行实时的流量监控，分析各种业务占用出口带宽的情况
用户监控和分析：
通过NetStream可以获得用户网络资源利用的详细情况，进而用于高效地规划以及分配网络资源，保障网络的安全运行。
1. 配置了NetStream功能的设备（即NDE网络数据导出器）把采集到的关于流的详细统计信息定期发送给NSC（网络流量收集器）；
2. 信息由NSC初步处理后发送给NDA（网络流量分析器）；
3. NDA对数据进行分析，以用于计费、网络规划等应用。
NetStream系统的工作过程如下：
通常情况下，数通产品在NetStream系统中担任NDE角色，NSC和NDA是专用的服务器

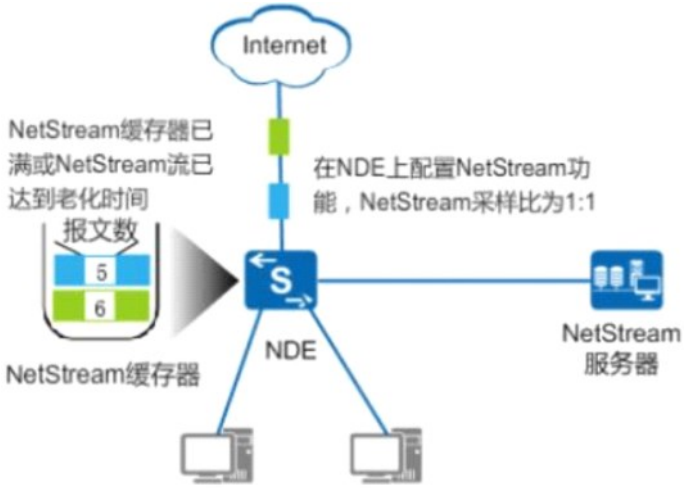
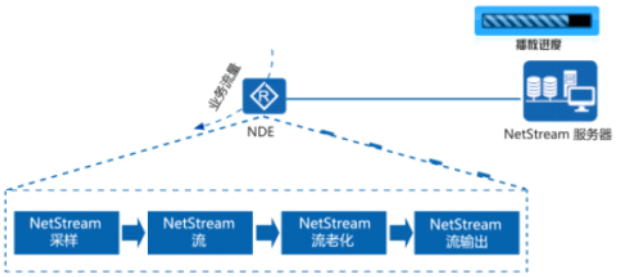


图2 NetStream功能原理图



如图2所示，配置了NetStream功能的设备（即NDE）业务流量正常转发。设备的NetStream模块按一定的采样方式进行NetStream采样，接下来对采样数据建立NetStream流，接着按一定的老化方式对流进行NetStream流老化处理，最后按一定的输出方式以及相应的版本进行NetStream流输出。至此，就完成了NDE设备最主要功能：把采集到的关于流的详细信息定期发送给NetStream服务器。

配置了NetStream功能的设备（即NDE）业务流量正常转发。设备的NetStream模块按一定的采样方式进行NetStream采样，接下来对采样数据建立NetStream流，接着按一定的老化方式对流进行NetStream流老化处理，最后按一定的输出方式以及相应的版本进行NetStream流输出。至此，就完成了NDE设备最主要功能：把采集到的关于流的详细信息定期发送给NetStream服务器。
采样方式：随机报文间隔采样、固定报文间隔采样、随机时间间隔采样、固定时间间隔采样
流老化方式（说白了就是啥时候从缓存器中发给服务器）：定时老化、强制老化、缓冲器满老化、 TCP连接中断触发老化

追问：如何理解Netstream流？
IPv4 NetStream会根据IPv4报文的目的IP地址、源IP地址、目的端口号、源端口号、协议号、服务类型ToS（Type of Service）、输入接口或输出接口来定义流，相同的七元组标识为同一条流；
IPv6 除了上面的七元组再增加一个流标签；
追问：Netstream各版本的差异？
版本5：根据七元组产生原始的数据流，但报文格式固定，不易扩展。
版本8：支持聚合输出格式
版本9：基于模板方式，可以用来灵活输出各种组合格式的数据
NetStream输出的报文主要有V5、 V8、 V9三个版本

交换机、路由器分别有哪些表项，如果不存在相应表项，数据如何处理 ；
分情况分析：
1、二层交换机----------只有MAC地址表
A、收到广播报文，广播域内泛洪
B、收到组播报文，正常情况下交换机未开启IGMP Snooping会在广播域内泛洪，所以建议开启IGMP Snooping避免上述情况
特殊情况：比如交换机关闭stp功能，交换机收到后丢弃发往0100-c200-0000的地址的组播流量会丢弃掉（默认不透传）
C、单播流量 ，已知单播帧转发、未知单播帧泛洪
2、三层交换机-------MAC地址表、 ARP表和路由表
三层转发原理
数据报文过来时，解析目标MAC地址：
如果为自身VLANIF接口的MAC地址则上送CPU查路由， 没有对应路由条目丢弃；
如果存在对应路由条目，则需要继续检查ARP表项封装数据，如果存在对应的ARP表项则直接封装二层转发数据
如果没有ARP表项，则需要进行ARP请求相应MAC地址
如果不为自身VLANIF接口的MAC地址 ，则根据MAC地址实现二层转发，如果mac地址表没有在广播域内泛洪
后续形成硬件转发表（一次路由多次交换）：对应的MAC 、 VLAN 、出接口 、 IP，实现快速转发
3、路由器------ARP、路由表 、如果增加二层交换模块会再多一个MAC地址表
查路由表，有路由条目进行转发，无路由条目就丢弃
如果存在路由条目，封装目标MAC地址的时候查ARP表进行封装，没有条目则进行ARP请求 ，如果请求不到丢弃
后续生成FIB实现硬件转发，转发流量直接查看fib表
注意：此处可以主动介绍FIB非0x0查标签的情况
注意：如果出口路由器通常存在NAT映射表项，如果没有对应表项则数据也会丢弃，再进一步就可能扯到NAT-ALG了
追问：
1、数据转发过程中的源目MAC、源目IP地址哪些会变化？
2、 IGMP Snooping的一些追问
3、 ARP代理的一些场景和追问-----结合文档仔细一点

园区网关放置
1、成本角度：
网关放置在汇聚层，接入层设备选型使用二层交换机即可，相对而言节约成本
网关放置在接入层，都需要选择三层设备，成本较高
2、集中控制角度：
网关放置在汇聚层，可以在汇聚层部署DHCP集中下发IP地址、部署相应的策略实现路由控制和选路、部署ACL实现安全管理
网关放置在接入层，如果需要集中部署DHCP则可能需要使用DHCP中继，否则只能分散在接入层交换机上；
并且不便于集中配置路由控制和选路、安全管理
3、 IP地址规划角度
网关放置在汇聚层，汇聚到接入只需要二层接入，无需规划额外的互联IP地址
网关放置在接入层，汇聚到接入之间也需要配置相应的IP地址实现互联，需要规划相应的IP地址
4、管理角度
网关放置在汇聚层，二层网络不需要运行路由协议，相应的维护的各类表项简单
网关放置在接入层，接入和汇聚之间也需要运行路由协议，维护的邻居表、链路状态数据库相对较多，增加管理成本
5、环路问题
网关放置在汇聚层，二层网络需要借助STP等协议实现防环，STP收敛较慢，建议使用RSTP或者MSTP进行优化
网关放置在接入层，接入层和汇聚层之间运行路由协议，所以无需二层防环，而路由协议本身也有对应的防环机制
6、冗余角度
网关放置在汇聚层，可以部署相应的VRRP实现网关的冗余，二层交叉双上联或者Eth-trunk提供链路冗余
网关放置在接入层，接入层设备只能通过部署堆叠等技术实现冗余，仍然可以用Eth-Trunk实现链路冗余
7、扩展角度
网关放置在汇聚层，新增接入交换机和终端只需要增加对应VLAN和配置接口即可，无需额外其他配置，扩展较为方便
网关放置在接入层，新增接入交换机和终端设备需要额外规划IP地址、设备互联及协议交互，相对较为复杂
8、广播域及设备表项角度
网关放置在汇聚层，二层广播域相对较大，汇聚交换机维护的MAC地址表和ARP表项条目较多
网关放置在接入层，广播域相对较小，MAC地址表项和ARP表项分散在接入层交换机
总结：
园区网/企业网----建议考虑管理维护是否方便、是否易于操作
数据中心网络------稳定、高效 、安全
1、数据中心网络趋于扁平化，接口密集程度高，将网关放置在接入层设备，可以根据不同业务分割广播域，降低广播风暴的可能，提升安全程度
2、数据中心网络发展，东西向流量（横向流量）增多，用于虚拟机迁移等业务，可以将网关置于接入层，减少去往汇聚层流量
追问：
1、二层、三层转发原理？

2、 VRRP优先级配置？
3、 MVRRP和MSTP？