目 录

NetStream

NetStream 技术应用背景 Internet 的高速发展为用户提供了更高的带宽，支持的业务和应用日渐增多，传统流量统计如 SNMP、端口镜像等，由于统计流量方式不灵活或是需要投资专用服务器成本高等原因，无法满足对网络进行更细致的管理，需要一种新技术来更好的支持网络流量统计。

NetStream 技术是一种基于网络流信息的统计技术，可以对网络中的业务流量情况进行统计和分析。在网络的接入层、汇聚层、核心层上，都可以通过部署 NetStream。

NetStream 技术的应用有以下几种。

- 计费：NetStream 为基于资源（如线路、带宽、时段等）占用情况的计费提供了精细的数据。Internet 服务提供商可以利用这些信息来实行灵活的计费策略，如基于时间、带宽、应用、服务质量等。企业客户可以使用这些信息计算部门费用或分配成本，以便有效利用资源。
- 网络规划：NetStream 可以为网络管理工具提供关键信息，比如各个 AS 域之间的网络流量情况，以便优化网络设计和规划，实现以最小的网络运营成本达到最佳的网络性能和可靠性。
- 网络监控：通过在出口部署 NetStream，对连接 Internet 网络的接口进行实时的流量监控，可以分析各种业务占用出口带宽的情况。网管人员可以根据这些信息判断网络的运行情况，尽早发现不合理的网络结构或是网络中的性能瓶颈，方便网管人员规划和分配网络资源。
- 用户监控和分析：通过 NetStream 技术可以使网络管理者轻松获取用户使用网络和应用资源的详细情况，进而用于高效地规划以及分配网络资源，并保障网络的安全运行。

NetStream 简介

NetStream 流定义

NetStream 是一项基于“流”来提供报文统计的技术。NetStream 支持二层报文、IP 报文（UDP、TCP、ICMP 报文）和 MPLS 报文的统计。

- 对于 IPv4 报文，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、ToS（Type of Service，服务类型）、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。
- 对于 IPv6 报文，IPv6 NetStream 会根据 IPv6 报文的目的 IP 地址、源 IP 地址、目的端口号、源端口号、协议号、流量分类、流标签、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。
- 对于 MPLS 报文，可以统计 MPLS 报文内的 IPv4/IPv6（6PE 情况下）信息。如果统计 IP 信息，此时会根据 MPLS 标签栈和 IP 信息共同确定一条流。

NetStream 的系统组成

一个典型的 NetStream 系统由 NDE、NSC 和 NDA 三部分组成。

- NDE（NetStream Data Exporter）

NDE 负责对网络流进行分析处理，提取符合条件的流进行统计，并将统计信息输出给 NDA（NetStream Data Analyzer）设备。输出前也可对数据进行一些处理，比如聚合。配置了 NetStream 功能的设备在 NetStream 系统中担当 NDE 角色。

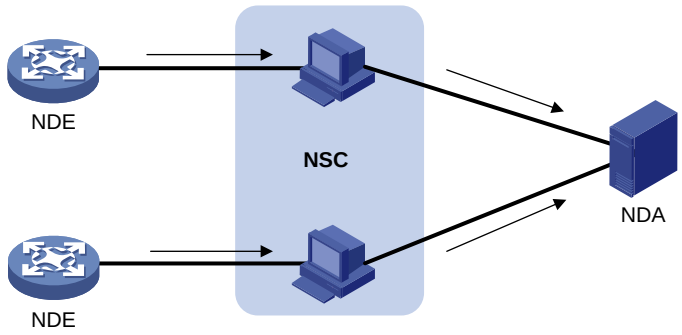
- NSC（NetStream Collector）

NSC 通常为运行于 Unix 或者 Windows 上的一个应用程序，负责解析来自 NDE 的报文，把统计数据收集到数据库中，可供 NDA 进行解析。NSC 可以采集多个 NDE 设备输出的数据，对数据进行进一步的过滤和聚合。

- NDA（NetStream Data Analyzer）

NDA 是一个网络流量分析工具，它从 NSC 中提取统计数据，进行进一步的加工处理，生成报表，为各种业务提供依据（比如流量计费、网络规划，攻击监测）。通常，NDA 具有图形化用户界面，使用户可以方便地获取、显示和分析收集到的数据。

图 1 NetStream 系统中的设备角色



如 图 1所示，NetStream进行数据采集和分析的过程如下：

(1) 配置了 NetStream 功能的设备（即 NDE）把采集到的关于流的详细信息定期发送给 NSC；

(2) 信息由 NSC 初步处理后发送给 NDA；

(3) NDA 对数据进行分析，以用于计费、网络规划等应用。

NetStream 关键技术

流老化

NetStream 流老化是设备向 NSC 输出流统计信息的一种手段。当设备启用 NetStream 功能后，流统计信息首先会被存储在设备的 NetStream 缓冲区中。当存储在设备上的 NetStream 流信息老化后，设备会把缓冲区中的流统计信息通过指定版本的 NetStream 输出报文发送给 NSC。

NetStream 流老化有以下三种机制：

- 按时老化
- 强制老化
- TCP 的 FIN 和 RST 报文触发老化。

1. 按时老化

按时老化分为以下两种方式：

- 不活跃的流老化：从最后一个报文开始，该流在指定的不活跃流老化时间内没有被采集到（即在设定的不活跃流老化时间内统计到的流数目没有增加），那么设备会向 NSC 输出该流的统计信息，这种老化称为不活跃的流老化。通过这种老化，可以清除设备上 NetStream 缓冲区中的无用表项，充分利用统计表项资源。
- 活跃的流老化：从第一个报文开始，该流在指定的活跃流老化时间内一直能被采集到。活跃时间超过设定的活跃流老化时长后，需要输出该流的统计信息，这种老化称为活跃的流老化。因为该流实际上还存在，所以在设备上 NetStream 缓冲区关于该流的统计表项本身仍然存在。这种老化方式是设备为了向 NSC 输出活跃流统计信息的一种机制。

2. 强制老化

执行强制老化命令，用户可以将 NetStream 缓冲区中所有流老化，并清除 NetStream 缓冲区信息。

3. TCP 的 FIN 和 RST 报文触发老化

对于 TCP 连接，当有标志为 FIN 或 RST 的报文发送时，表示一次会话结束。因此当一条已经存在的 TCP 协议 NetStream 流中流过一条标志为 FIN 或 RST 的报文时，可以立即老化相应的 NetStream 流。但是假如一条流的第一个报文就是 TCP 的 FIN 或 RST 报文，则会按正常的流程创建一条新流，不进行老化。

流输出

1. 普通流输出

普通流输出是指所有流的统计信息都要被统计，并且每条流的统计信息都要输出到 NSC 设备。

普通流的优点是：NSC 可以得到每条流的详细统计信息。但是缺点也是很明显的，这种方式增加了网络带宽和设备的 CPU 占有率，而且为了存储这些信息，需要大量的存储介质空间。并且很多情况下，用户并不需要获取所有流的统计信息。

2. 聚合流输出

(1) IPv4 NetStream 聚合功能

聚合流输出是指采用聚合流输出功能后，设备对与聚合关键项完全相同的流统计信息进行汇总，从而得到对应的聚合流统计信息，并且将该聚合统计信息发送到相应的接收聚合统计信息的 NSC 设备。

例如，如 表 1所示，发送四条TCP流，其目的地址相同、源地址不同，源端口、目的端口均为 10，选择“协议-端口聚合”方式，该聚合方式的依据为“协议号、源端口、目的端口”，因为这四条TCP流的源端口、目的端口和协议号相同，在聚合流统计表项中只会记录一条聚合流统计信息。设备只将聚合统计信息发送给相应的接收聚合统计信息的NSC，由此可见，聚合的最大好处是可以减少对网络带宽的占用。

在目前的实现中，IPv4 NetStream聚合流输出支持的 12 种方式如 表 1所示。

表 1 NetStream 的 12 种聚合方式

聚合方式	聚合关键项
自治系统聚合	源 AS 号、目的 AS 号、输入接口索引、输出接口索引
协议-端口聚合	协议号、源端口、目的端口

聚合方式	聚合关键项
源前缀聚合	源 AS 号、源掩码长度、源前缀、输入接口索引
目的前缀聚合	目的 AS 号、目的掩码长度、目的前缀、输出接口索引
源和目的前缀聚合	源 AS 号、目的 AS 号、源掩码长度、目的掩码长度、源前缀、目的前缀、输入接口索引、输出接口索引
前缀端口聚合	源前缀、目的前缀、源掩码长度、目的掩码长度、ToS、协议号、源端口、目的端口、输入接口索引、输出接口索引
服务类型-自治系统聚合	ToS、源 AS 号、目的 AS 号、输入接口索引、输出接口索引
服务类型-源前缀聚合	ToS、源 AS 号、源前缀、源掩码长度、输入接口索引
服务类型-目的前缀聚合	ToS、目的 AS 号、目的掩码长度、目的前缀、输出接口索引
服务类型-前缀聚合	ToS、源 AS 号、源前缀、源掩码长度、目的 AS 号、目的掩码长度、目的前缀、输入接口索引和输出接口索引
服务类型-协议-端口聚合	ToS、协议类型、源端口、目的端口、输入接口索引、输出接口索引
服务类型-BGP 下一跳聚合	ToS、BGP 下一跳地址、输出接口索引

(2) IPv6 NetStream 聚合功能

在目前的实现中，IPv6 NetStream聚合流输出支持的 6 种方式如 表 2所示。

表 2 IPv6 NetStream 的 6 种聚合方式

聚合方式	聚合关键项
自治系统聚合	源 AS 号、目的 AS 号、输入接口索引、输出接口索引
协议-端口聚合	协议号、源端口、目的端口
源前缀聚合	源 AS 号、源掩码长度、源前缀、输入接口索引
目的前缀聚合	目的 AS 号、目的掩码长度、目的前缀、输出接口索引
源和目的前缀聚合	源 AS 号、目的 AS 号、源掩码长度、目的掩码长度、源前缀、目的前缀、输入接口索引、输出接口索引
BGP 下一跳聚合	BGP 下一跳地址、输出接口索引

输出报文的版本格式

目前 Netstream 输出的报文主要有 5、8、9 三个版本。其中版本 9 可以为用户提供根据实际需求设计各种统计元素的模板，使统计信息的输出更为灵活。

- 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，但报文格式固定，不易扩展。
- 版本 9：基于模板方式，使统计信息的输出更为灵活，可以用来灵活输出各种组合格式的数据。版本 9 支持对 BGP 下一跳、MPLS 等统计输出。

说明

IPv6 Netstream 输出的统计信息只能使用版本 9 格式。

NetStream 采样过滤功能

NetStream 采样

IPv4 NetStream 可以与 Sampler 采样器配合使用。通过设定适当的采样间隔，不但减少了统计的报文数量，收集到的统计信息也可以保证基本正确地反映整个网络流的状况。另外，采样还可以减小对设备转发性能造成的影响。

NetStream 过滤

IPv6 NetStream 可以与 ACL（Access Control List，访问控制列表）和 QoS（Quality of Service，服务质量）配合使用，NetStream 只统计符合 ACL 和 QoS 筛选出的特定报文。通过这种方式可以使 NetStream 对用户关注的数据进行统计，更能满足用户多样的统计要求。

NetStream 无论是和 ACL 或是和 QoS 配合使用，都是为了先对数据流进行过滤，这样 NetStream 就可以“只对某些符合条件的流”进行统计。两者方式的区别是：QoS 可以更加灵活的指定流，且应用方式多样。