网络流量监测技术及性能分析

杨 策[1]，张永智[2]，庞正社[2]
(1. 西安电子科技大学 信息科学研究所，陕西 西安 710071；2. 空军工程大学 电讯工程学院，陕西 西安 710077)

摘 要：网络流量数据对网络的资源分布、容量规划、服务质量分析、错误监测与隔离、安全管理都十分重要，文中论述了网络流量监测技术的模型与实现，然后对3种主要网络流量监测技术的特点和功能进行了比较和分析。最后，给出了3种技术的不同适用场合。

关键词：流量监测；网络管理；RMON；NetFlow；sFlow
中图分类号：TN913.2　　**文献标识码**：A　　**文章编号**：1009-3516(2003)01-0057-04

网络流量监测是网络管理和系统管理的一个重要组成部分，网络流量数据为网络的运行和维护提供了重要信息。这些数据对网络的资源分布、容量规划、服务质量分析、错误监测与隔离、安全管理都十分重要。

1 网络流量监测技术

1.1 网络流量监测系统模型

为获取交换式网络的流量信息，要对交换机的每个端口进行监测。但交换机和路由器内部的数据流也是影响网络性能的一个重要因素，因此，单纯对端口进行监测并不能完全反映网络的流量信息，可行的解决办法是在交换机和路由器的内部用Agent(代理)对所有数据流进行监测。

网络流量监测系统的模型如图1所示，一般由Agent、流量分析服务器和网络应用程序3部分组成。目前网络流量监测技术主要有3种：RMON、NetFlow和sFlow。

1.2 RMON (Remote Monitor)

RMON是IETF(因特网工程任务组)制定的一种支持远程、异构网络体系的流量监测标准，它是对SNMP网络管理体系的重要补充。通过在每一子网安置一个RMON探测设备(RMON Probe，或RMON Agent)，来实现对该网段的流量进行监测和分析，解决了在互联网环境下进行网络管理的难题。

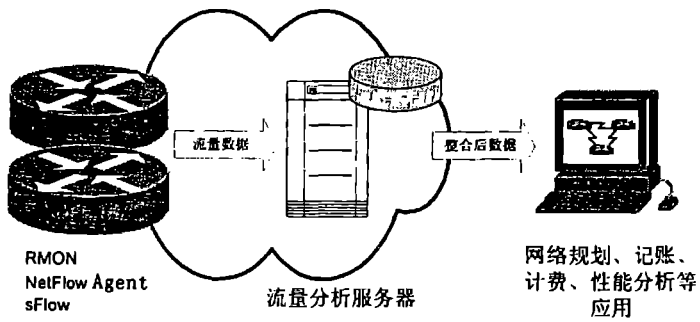

图1 网络流量监测系统模型

RMON Agent在对网络流量进行监测的同时还对每一个数据包进行复制、解包，并把有关信息记录到数据库的相关表中，这些数据可被网络管理站(流量分析服务器)定期下载。

1.3 NetFlow

NetFlow是Cisco公司的专有技术，广泛应用于Cisco的路由器和交换机中。它提供高性能的第三层交换技术，可以用来捕获、显示和分析各种网络数据流信息，并把这些网络流量信息发给流量分析服务器(NetFlow FlowCollector)。

具备NetFlow功能的网络设备对经过的每一个IP数据包进行解包，生成并维护相关数据库(内容包括

收稿日期：2002-06-03
作者简介：杨 策(1975-)，男，陕西西安人，硕士生，主要从事网络管理和性能分析研究.

经过该设备的每一条动态数据流)并定期以 UDP 数据包的形式发送给流量分析服务器。

1.4 sFlow

sFlow 是 InMon 公司提出的一种网络流量监测技术,已提交给 IETF 并以 RFC 3176 文件的形式进行了发布。sFlow 通过对交换机或路由器处理的数据包进行周期性采样来获取网络流量信息,然后把采样数据包发送给流量分析服务器(sFlowCollector)。

sFlow 的采样过程用 ASIC(专用集成电路)实现,速度非常快,可达 10Gbps 甚至更高,真正实现线速处理。它除了可对数据包作第三层(IP 层)分析外,还可以进行第二层(MAC 地址或 VLAN 标识)的分析和处理。

2 技术分析

2.1 Agent 对网络设备资源的占用

3 种流量监测技术都要通过 Agent 以嵌入式系统来实现,下面通过 Agent 对网络设备的 CPU、内存和带宽 3 大资源的占用情况进行性能分析。

2.1.1 CPU

交换机和路由器有许多端口,而且内部交换的数据量非常大,所以对网络流量进行监测需要进行大量的计算,这就要求其 CPU 有很强的计算能力。

RMON Agent 要对网络中的每个数据包逐个进行解包分析,并把结果插入数据库的有关表中。Agent 不但要对网络管理站定期的轮询请求进行处理,还要把流量数据按照 ASN. 1 的格式进行编码,以 SNMP 数据包发给网络管理站。

NetFlow Agent 也要对每一个数据包进行解包分析并把结果插入数据库的有关表中,以 UDP 数据包发给指定地址的流量分析服务器。

sFlow Agent 用硬件技术完成对数据包的采样并转发给流量分析服务器,它对 CPU 的负荷是最低的。假设网络链路的速率为 200 000 个数据包/秒,采样率为 1/1000,CPU 处理能力只需达到 200 个数据包/秒即可。

采用 RMON 和 NetFlow 技术的 Agent 都试图对交换机和路由器所转发的数据包逐个进行解包和分析,并以此在内存中建立网络流量矩阵。随着网络中流量模式的变化,流量矩阵也会不断变化。这都会对 CPU 的负荷产生不可预料的影响,甚至可能因此导致整个系统崩溃。

图 2 是这 3 种流量监测技术对 CPU 资源占用情况的比较。显然,RMON 最高,其次是 NetFlow,而 sFlow 最低。

2.1.2 内存

对网络流量进行监测,内存大小对 Agent 至关重要。内存过小,会造成 Agent 流量监测进程溢出,导致系统崩溃、数据丢失;内存过大,会使网络设备的成本造成不必要的增加。

RMON Agent 必须在内存中保存网络流量矩阵的全部内容,并在等待向网络管理站发送这些数据的同时,为新一轮的流量监测建立一个新的数据库。

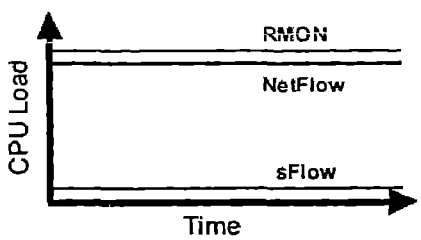

图 2 对 CPU 资源占用比较

NetFlow Agent 的数据库会定期根据网络数据流的状况自动更新,防止内存溢出。

RMON Agent 和 NetFlow Agent 都要在内存中建立网络流量交换矩阵,其大小同网络中流量模式密切相关。在最坏情况下,每一数据包都代表一条新数据流,它的地址和计数器等信息都在数据库中单独存储。sFlow Agent 的内存空间只需容纳一个数据包即可。因为每一次数据采样结束时,该数据包会被立即转发给流量分析服务器。

图 3 是这 3 种流量监测技术对内存需求的比较。RMON Agent 对内存要求最高,约 8 ~ 32 MB。NetFlow Agent 对内存要求较高,大概需要 4 ~ 8 MB。而 sFlow Agent 对内存要求最低,只需要 1 kB。

2.1.3 带宽

将获得的流量数据由 Agent 传给流量分析服务器,不但会消耗一定的网络带宽,而且会对正常的网络应用造成一定的影响,高峰值的突发数据传输会在网络中造成明显的拥塞。

图 4 是这 3 种流量监测技术对网络带宽占用的比较。

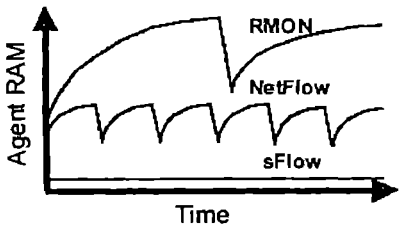

图 3　内存需求比较

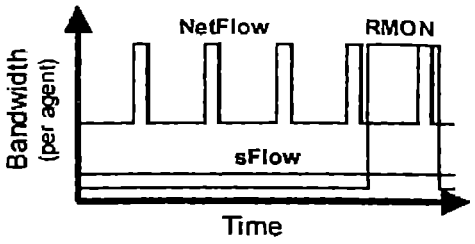

图 4　带宽占用比较

RMON Agent 在服务器轮询时带宽占用低,在给服务器发送 SNMP 数据包时有很大的突发数据传输,会给流量分析服务器造成周期性的影响。

NetFlow Agent 当 1 条数据流结束或为容纳新产生的数据流信息,通过对内存周期性的刷新来开辟出新的自由空间时,有较大的突发数据传输。

sFlow Agent 对带宽占用小而平滑,没有大的数据突发。因为其数据采样过程产生的是 1 个恒定的数据流,所以流量分析服务器接收到的各个 sFlow Agent 传来数据量的总和也是 1 个稳定值。

因而,从带宽和突发性来看,sFlow 技术都优于其它两种流量监测技术。

2.2　Agent 对流量分析服务器资源的占用

流量分析服务器的资源占用情况反映了每一台服务器可管理 Agent 的数目和整个网络流量监测系统的成本和可度量性。

NetFlow Agent 对服务器的资源占用最高。虽然服务器只接收数据,但数据量最大。因为 NetFlow Agent 返回的流量矩阵数据比 RMON 要详细,所以服务器进行数据整合时要花费更多的资源。

RMON Agent 对服务器的资源占用较高。它采用 SNMP 协议进行状态轮询和数据采集,服务器发出和接收的数据几乎相等。但未经采样的网络流量矩阵数据量非常大,服务器整合各节点发来的数据仍是一项艰巨的任务。

sFlow Agent 对服务器的资源占用最低。因为服务器得到的是采样后的流量数据,比前面两种流量矩阵的数据量都要小得多。此时服务器主要接收数据,仅发出少量数据。

2.3　性能分析

2.3.1　网段流量实时统计

对网络的每一条链路的流量进行实时追踪和趋势预测是网络管理系统的一项基本功能。

RMON 支持这一基本功能。但是服务器必须使用 SNMP 协议对所有的 Agent 进行轮询,这就限制了每一台服务器所能管理的 Agent 的个数。

NetFlow 没有明确定义该项功能,但是服务器可以通过 SNMP 协议来得到大部分网络设备的流量信息,方法和 RMON 相同。

sFlow 也支持这一基本功能。服务器不需要轮询,可随时从每一个 Agent 发来的数据包中得到该信息。因为端口计数信息已通过编码携带在每个传回的采样数据包里。

2.3.2　最繁忙网络节点实时认定

RMON 支持最繁忙网络节点实时认定功能。但服务器必须进行轮询,这个条件限制了每一台服务器所能管理 Agent 的个数。

NetFlow 不支持该项功能。

sFlow 支持该项功能,服务器可从每一个 Agent 传回的采样数据包中得到所需信息。

2.3.3　流量矩阵生成

基于节点的流量矩阵反映了网络中流量的瞬时状态,它对网络的容量规划、计费、拓扑优化等尤其重要。

RMON 提供了扩展套件来生成网络流量矩阵,但 RMON Agent 是否有足够的内存来同时容纳这些数据是个问题。另外,每次为支持 1 种新的网络协议,都要对 Agent 的程序进行升级。

NetFlow 支持该项功能,但是只支持 IP 、ICMP、TCP 和 UDP4 种格式的数据包。

sFlow 同样支持该项功能,支持的数据包类型多达 10 余种,包括了目前各种主要的网络协议,如 IPv4、IPv6、IPX、AppleTalk 和 Ethernet 等。

3 结论

通过对 3 种网络流量监测技术和性能的分析,可以得出以下结论:

RMON 技术适合进行远程协议分析。具有包过滤、包捕捉、解包等功能,可用于网络错误分析。尤其当需要深入了解每个数据包中网络协议的时戳和包序列号时,RMON 显得较为合适。

NetFlow 适用于要求准确记录每一条数据流的场合,如对路由器的中速 WAN 链路进行计费和安全监测。但由于 NetFlow 会产生详尽的数据流信息,所以每个服务器可管理的链路有限,最多只能管理 10 条左右。

sFlow 采用了对数据包进行统计采样的技术,它能管理的 Agent 的数目大为增加,每个服务器甚至能管理成千上万个端口。它适用于具有高密度端口的设备或对高速干线链路进行监测、计费和安全管理,但硬件成本较高。

参考文献:

[1] Mani Subramanian. 网络管理——原理与实践(影印版)[M]. 北京:高等教育出版社,2001.

[2] Tanenbaum A S. Computer Network 3d ed [M]. Prentice Hall PTR ,1996.

[3] Stallings, William. SNMPv2 SNMPv3 and RMON[M]. Addison - Wesley,1998.

(编辑:门向生)

Network Traffic Monitoring Techniques and Analysis of Performances

YANG Ce[1], ZHANG Yong - zhi[2], PANG Zheng - she[2]

(1. Information Science Institute, XiDian University, Xi'an, Shaanxi 710071, China; 2. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: Network traffic data is very important to the network resource distribution, plan of netwrok capacity, analysis of network service quality, network error monitoring and isolation, and management of network security. This paper first discusses the model and implementation of network traffic monitoring techniques, and then presents the comparison among and analysis of the three kinds of main network traffic monitoring techniques, finally intrduces the different applicable situations of the three kinds of techniques.

Key words: traffic monitoring; network management; RMON; netflow; sFlow