

文章编号:1001-9081(2006)04-0961-02

基于 SNMP 的远程网络拓扑发现方法

周 智,寇晓葵,罗军勇

(信息工程大学 信息工程学院,河南 郑州 450002)

(xjzhouzhi@163.com)

摘 要:提出并实现了基于简单网络管理协议(SNMP)的大型异构 IP 网络拓扑发现方法,该方法包括代理发现、拓扑信息探测和拓扑信息分析三个步骤。对代理发现中的探测报文构造、去除冗余信息、信息分析算法以及非转发设备信息利用等关键问题进行了讨论,针对探测时遇到的路由器间歇性不响应、路由器过长时间不响应和探测目标为子网地址等问题进行了分析并给出了解决方案。工程实现结果表明,该方法可以高效地获取较为丰富的拓扑信息,与 traceroute 路径探测结合使用,可以极大地提高拓扑发现结果的完整性。

关键词:简单网络管理协议;远程网络拓扑发现;Internet 控制消息协议

中图分类号: TP393.02 **文献标识码:** A

A SNMP-based algorithm for remote network topology discovery

ZHOU Zhi, KOU Xiao-rui, LUO Jun-yong

(Information Engineering College, Information Engineering University, Zhengzhou Henan 450002, China)

Abstract: A kind of SNMP-based method was proposed to discovery large-scale heterogeneous IP network topology, which includes Agent discovery, topological data collection and analysis. The main idea in the process of Agent discovery such as construction of packet, eliminate redundant data, analyse algorithm and using not-forwarding device-based data was discussed. A solution was given to the intermittent router non-responsiveness, prolonged router non-responsiveness and net numbet-based target address. The result of the experiment illustrates that the method can capture amount of topology information efficiently. Unit SNMP with traceroute can improve the integrity of topology discovery obviously.

Key words: SNMP; remote topology discovery; ICMP

0 引言

网络拓扑发现旨在发现网络实体,并获取实体间的连接关系。传统的拓扑发现作为网络故障定位、网络仿真、网络管理、通信瓶颈分析和网络性能分析的前提与基础,其目的是获取网络三层拓扑和二层拓扑。其中三层拓扑指三层设备(包括路由器和三层交换设备)与子网以及三层设备之间的连接关系。二层拓扑指以交换机为主的两层设备之间,以及交换机与终端间的连接关系。近年来,随着互联网规模的急剧膨胀,研究大型 IP 异构网络,甚至整个互联网的拓扑已成为一个热点^[1~3],其结果被广泛应用于模拟仿真、协议设计和防范大规模网络攻击等领域。

对于大型 IP 异构网络而言,由于受到时间、安全、空间和跨管理域等因素的影响,网络拓扑发现一般是获取 IP 层拓扑和 AS(Autonomic Systems,自治系统)层拓扑,其中 IP 层拓扑指利用 IP 地址标识的网络设备之间的连接关系,AS 层拓扑则是 AS 之间的连接关系。对于获取 AS 层拓扑而言,常用的方法是基于 IP 层拓扑进行推导,而获取 IP 层拓扑的基本方法是基于 ICMP 的 traceroute 路径探测^[1]。由于使用 traceroute 技术仅能发现树型结构,文献[2]在使用基本技术的基础上,对源路由进行分析,控制探测包的方向以发现交叉链路。文献[1]则采用了分布式的探测结构,从多个探测点

收集信息,以增强结果的完整性并提高探测效率。

利用基于 ICMP 的路径探测技术实施拓扑发现存在以下问题:

1)利用路径探测技术发现的路由器 IP 地址很可能是同一路由器设备的多个接口地址。为此,文献[1]使用了基于 ICMP 端口不可达报文的别名探测技术,对同一设备的别名进行归并。但是,由于不是每个路由器都会由近端接口向探测源返回一个端口不可达报文,再加上有时由于发包量的增加,路由器会丢弃相同类型数据包不予处理和回应,其别名归并结果的完整性是值得置疑的。

2)为了防范 DDoS 攻击,目前大部分网络设备加入了“ICMP limit”配置^[3],限制 ICMP 报文的发送速率,或者直接屏蔽 ICMP 报文,因此,基于 ICMP 的路径探测技术在实际中会遇到诸多限制,在很多情况下无法得到结果。

3)基于 ICMP 的路径探测技术需要对每一跳都发送探测报文,其探测流量是非常巨大的,对于探测大型目标而言,这种流量的影响是不可忽略的。

本文使用 SNMP 技术进行拓扑发现。SNMP 相关探测技术被广泛应用于网管软件中的拓扑发现^[4~8]。经实际测试发现,SNMP 在远程网络拓扑发现中也能够获得比较丰富的结果。此外,使用 SNMP 的优势在于只要针对少量设备发送探测报文,探测速度快,探测流量小。

收稿日期:2005-10-31;修订日期:2006-01-08 基金项目:国家 863 计划项目资助(2001AA146010)

作者简介:周智(1977-),女,四川泸州人,初级工程师,硕士研究生,主要研究方向:计算机网络结构与与设计;寇晓葵(1978-),女,河北晋州人,讲师,博士研究生,主要研究方向:网络安全;罗军勇(1964-),男,江西南昌人,副教授,硕士,主要研究方向:计算机软件与理论及信息安全。

在使用 SNMP 探测时,引入了 SNMP 代理发现技术,除使用路由器代理外,还有效地利用了主机代理,此外,探测过程中会遇到路由器间歇性不响应或过长时间不响应和探测目标为子网路号的问题,本文对这些问题也进行了论述。

1 网络拓扑发现的思路及实现步骤

对于利用 SNMP 进行网络拓扑发现的算法而言,传统的方式是先找一个种子,以此为起点取得种子的路由表,从路由表中获取其他种子的路由信息,将其他种子路由加入路由链表后进行广度或深度优先遍历^[1]。而对于发现大型异构 IP 网络而言,目标内支持 SNMP 的设备是未知的。因此,首先对目标网段地址进行扫描,以发现其中开放 SNMP 的设备,即 SNMP 代理;再探测得到 SNMP 代理的 IP 表和 route 表;最后对结果进行综合分析。整个过程包括以下三个步骤:

1.1 SNMP 代理发现

SNMP 代理发现的基本思想是向目标网段的每个地址的 161 端口发送 SNMP 的 GetRequest 报文,若收到 SNMP 的 GetRequest 报文,则此网络设备的 SNMP 服务可用,将其加入代理链表。为了提高效率,在报文构造时封装变量如下: sysDescr(设备描述); sysName(设备名称); sysServices(服务类型); ifNumber(设备接口数); ipForwarding(设备转发类型); ipAdEntAddr(接口 IP 地址); ipAdEntNetMask(接口子网掩码)。

其原因如下:

1) 对于判断网络设备是否为路由器而言, ipForwarding 等于 1 是必须的条件,但是只有这一个不够充分。如普通装上 Windows 2000 的 PC 和配置为代理服务器的 PC 其 ipForwarding 也是 1,所以加入 ifNumber 值大于 1 加以确认。但对于配置为代理服务器的 PC 而言,其 ipForwarding 等于 1,且 ifNumber 值大于 1,此时再加入 sysServices 进一步确认。若是主机则其 sysServices 为 72。

2) 实际网络环境下,当一个路由器的多个接口地址都处于同一个探测范围时,则该路由器会有多个接口地址对探测报文进行回应。为了避免将这些别名地址作为不同的路由器进行重复探测,要对同一路由的多个回应地址进行归并操作。此时引入 sysDescr、sysName 和 ifNumber 对路由器进行归并。

3) 相同的设备在缺省条件下使用时, sysDescr、sysName 和 ifNumber 这三项都是相同的,所以在路由器归并时还需要加上 ipAdEntAddr 和 ipAdEntNetMask,根据 IP 地址表第一项的配置是否相同来判断是否是同一个路由器。

在探测过程中通过对以上参数的判断,可以得到不重复的代理,并且可以区分设备是转发设备还是非转发设备,为进一步探测和分析奠定了基础。

1.2 拓扑相关信息探测

获得拓扑信息主要是通过读取网络设备的路由表,需要读取的关键信息如下,对这些关键信息的使用将在拓扑相关信息分析中进行说明:

对于 IP 地址表来说,需要取得的数据为: ipAdEntIfIndex(接口索引); ipAdEntAddr; ipAdEntNetMask。

对于 IP 路由表来说,需要取得的数据为: ipRouteIfIndex(接口索引); ipRouteType(路由类型); ipRouteNextHop(接口的下一跳 IP 地址); ipRouteDest(目的 IP 地址)。

在实际网络环境中,转发设备的 IP 地址表和 IP 路由表往往很大,多至几百上千条记录,为了提高后期分析的效率,

取路由表的时候要对冗余条目及无用条目进行过滤。具体有以下几种情况:

1) 在分析过程中 ipRouteType 为 3(direct)或 4(indirect)是有用的数据,但 ipRouteType 也可能被设置成 1(other)或 2(invalid)。因此,在取数据时,要对此类无用数据进行过滤。

2) 环回地址在分析过程中也是无效的,例如 ipAdEntNetMask 或 ipRouteDes 为 127.0.0.0 或 127.0.0.1,此类地址需要在探测时进行过滤。

3) 还有一些根据其所在子网地址明显能够发现是无用的条目,例如 ipAdEntAddr 或 ipRouteMask 为 0.0.0.0。

1.3 拓扑相关信息分析

对于同一个网络设备而言,各表中 index 相同的表项表示的是同一接口的各项属性。基于此,对探测得到的信息从以下三个方面进行分析:

1) 获得网络设备的接口信息(别名信息)

将 IP 地址表中的 ipAdEntAddr 和 ipAdEntNetMask 相与,可以得到每个接口 IP 对应的子网路号。这样就可以得到路由器的基本信息,即路由器的接口索引、接口 IP、接口的子网掩码和子网路号。

2) 分析获得网络设备间的连接关系

对网络设备间的连接关系,最终需要获得的数据如下:

ipAdEntAddr; ipAdEntNetMask; 子网路号; 与本接口直连的其他路由器的接口地址。

其中接口 IP 地址、子网掩码和子网路号可以由步骤 1(1.1 节)分析获得,与接口直连的路由器接口地址则由 IP 地址表和 IP 路由表综合分析获得,其分析过程如下所示:

对于 IP 路由表中的数据来说,当 ipRouteType 为 3 时,表示经过下一跳可直接到达 ipRouteDest 所标识的子网。用 IP 地址表的 ipAdEntIfIndex 与 IP 路由表的 ipRouteIfIndex 相匹配,找到与 ipAdEntAddr 对应的 ipRouteDest。

当 IP 路由表中的 ipRouteType 为 4 时,经过下一跳不能直接到达 ipRouteDest,但 ipRouteNextHop 为与 ipRouteIfIndex 所标识的接口直连的其他路由器的接口地址。用 IP 地址表的 ipAdEntIfIndex 与 IP 路由表的 ipRouteIfIndex 相匹配,找到与 ipAdEntAddr 对应的 ipRouteNextHop。

通过以上的分析可以得到路由器的连接关系,直连到子网的接口可以得到其子网路号,与路由器直连的接口可以得到相连路由器的接口地址。

3) 有效利用非转发设备

在逻辑拓扑传统探测方法中,通常会忽略非转发设备中的路由信息。但在实际探测中发现,非转发实体信息中有很大一部分可以作为逻辑拓扑探测的补充信息。出于安全,管理员可能会更改关键设备的一些配置,此时,若 ipForwarding 值为 2 的非转发实体的路由表中有到此关键设备的连接,则通过此非转发实体的路由表可以得到此关键设备的一个接口 IP,并能通过 IP 地址表得到此转发设备接口的子网掩码和子网路号。在处理的过程中,同时比对已经得到的连接关系,若此连接关系已经存在,则对冗余信息进行归并,否则将此连接关系作为已得逻辑拓扑的补充。

通过以上的分析可以比较完整地得到目标地址路由器之间的逻辑拓扑。

2 问题及解决方案

要分析出正确的拓扑结构,探测结果的完整性是很重要的

(下转第 973 页)

- [C]. 1988. 109 – 116.
- [2] PATTERSON DA, CHEN PM, GIBSON G, *et al.* Introduction to redundant arrays of inexpensive disk (RAID) [A]. Proceedings of IEEE COMPCON[C]. 1989. 112 – 117.
- [3] CHEN PM, LEE EK, GIBSON G, *et al.* Patterson, RAID: High Performance, Reliable Secondary Storage[J]. ACM Computing Surveys, 1994, 26(2): 145 – 185.
- [4] HELLERSTEIN L, GIBSON G, KARP R, *et al.* Coding techniques for handling failures in large disk arrays[J]. Algorithmica, 1994, 12(2/3): 182 – 208.
- [5] MACWILLIAMS FJ, SLOANE NJA. The Theory of Error-Correcting Codes[M]. North-Holland, Amsterdam, 1977.
- [6] GIBSON GA, HELLERSTEIN L, KARP RM, *et al.* Paterson, Failure Correction Techniques for Large Disk Arrays[A]. International Conference on Architectural Support for Programming Language and Operating System[C]. 1989. 123 – 132.
- [7] PARK C. Efficient placement of parity and data to tolerate two disk failures in disk array system[J]. IEEE Transactions Parallel and Distribute Systems, 1995, 6(11): 1177 – 1184.
- [8] CHIH-SHING TAU, TZONE-I WANG. Efficient Parity Placement Schemes for Tolerating Triple Disk Failures in RAID Architectures [A]. Proceedings of the 17th International Conference on Advanced Information Networking and Applications(AINA'03) [C]. 2003. 132 – 138.

(上接第962页)

的基础。在实际探测过程中我们发现,以下现象会影响结果的完整性:1)路由器间歇性不响应或过长时间不响应;2)探测目标为子网络号。

2.1 路由器间歇性不响应或过长时间不响应

在实际探测中发现,如果发送 SNMP 探测报文速率过大,那么大部分路由器节点会停止响应,即路由器的报文抑制现象。产生这种现象的原因在于路由器的转发机制设计中,限制了源节点发送报文的最小时间间隔或其可用的最大带宽。在实际实现中,一种实现方式是对探测报文进行排队,这样会产生路由过长不响应的现象;而另一种实现方式则会简单丢弃探测报文,这样会产生路由器间歇性不响应的现象。

从探测角度而言,由于使用了多线程机制并行探测,短时间内若对同一网段发送大量探测报文,就很容易触发路由器报文抑制。因此必须引入报文发送速率调节机制以避免触发报文抑制。在解决该问题时,采用了两种机制。在发现 SNMP 代理时使用目标分散机制,在对代理进行拓扑信息探测时使用指数退避机制。

1) 目标分散机制

①设 A 为目标地址空间内所有 IP 地址的集合,可表示为:

$$A = \{a \mid a = "x_1x_2x_3x_4", 0 \leq x_1, x_2, x_3, x_4 \leq 255\}$$

②以 m 为粒度将 A 划分为 n 个小集合,得到 $A_1, \dots, A_i, \dots, A_n$, 每个小集合可表示为:

$$A_i = \{a_1^{(i)}, a_2^{(i)}, \dots, a_m^{(i)} \mid a \in A, m \in N\}$$

则有 $A_i \subseteq A$ 。其中当 $i = n$ 时:

$$A_n = \{a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)} \mid a \in A, 1 \leq k \leq m, m \in N\}$$

③每个线程在探测时都从 n 个集合中各取一个元素,即线程所取目标集合为:

$$T_i = \{a_i^{(1)}, a_i^{(2)}, \dots, a_i^{(n)} \mid a_i^{(1)} \in A_1, \dots, a_i^{(n)} \in A_n, 1 \leq i \leq m\}$$

这种实现方式能够保证在同一段时间内探测源不会对同一网段发送大量的探测报文。这样能够避开路由器的报文抑制,有助于获得更多、更完整的拓扑信息。

2) 时间指数退避机制

在探测报文发出后,若在指定的超时时间内没有收到回应报文,则在重传时超时时间间隔以 2 的指数级增加,直至到达超时的最上限,若目标地址还不回应,则将此地地址设为永久不回应,越过此地地址继续处理下一个目标。

2.2 探测目标为子网络号

由于输入参数是未知的大段地址,所以在目标地址集合

中常会出现子网络号,此时根据网络的不同配置有以下几种可能的情况。

1)子网中的所有活动设备都不作回应,此时可直接越过此地地址处理下一个目标。

2)子网中的所有活动设备都以子网络号为 IP 地址回应探测报文。因为在拓扑结构中不能用子网络号作为网络设备的标识,所以要去除此类回应。

3)子网中的所有活动设备都以自身的 IP 地址回应探测报文。接收所有的回应报文,并加以分析,一次就可以获取子网内的所有活动设备。

3 结语

本文论述了基于 SNMP 获取大型 IP 异构网络拓扑的改进方法,该方法包括 SNMP 代理发现、拓扑信息探测和拓扑信息分析三个步骤。在代理发现过程中,考虑了报文变量选取、别名归并等问题,为后期的探测奠定了基础;在探测分析过程中,有效利用了非转发设备的路由信息,使探测结果更加完整。此外在实际测试中还发现了路由器间歇性不响应及目标地址为子网络号的问题,并通过分析给出了相应的解决方法。

在工程实现中,因为有共同体名的限制,SNMP 获得的结果不是很完整,可以结合 traceroute 的探测结果进行分析能够比较完整地获得路由器的各接口信息及连接状态,保证网络拓扑图的连通性和完整性。

参考文献:

- [1] SIAMUALLA R, SHARMA R, KESHAY S. Discovering Internet Topology[EB/OL]. <http://www.cs.cornell.edu/skeshav/papers/discovery.pdf>, 2005.
- [2] GOVINDAM R, TANGMUNARUNKIT H. Heuristics for Internet Map Discovery[A]. IEEE INFOCOM 2000[C]. 2000.
- [3] WADDINGTON DG, CHANG FZ, VISWANATHAN R, *et al.* Topology Discovery for Public IPv6 Networks[DB/OL]. ACM SIGCOMM Computer Communications Review, 2003.
- [4] 丘建林,何鹏.一种改进的网络拓扑发现方法[J].计算机应用, 2005, 25(4): 891 – 893.
- [5] 李玉鹏,王换招,田海燕,等.基于 SNMP 和 Java 的网络拓扑发现[J].计算机工程与应用, 2004, 40(5): 152 – 154.
- [6] 肖宗水.链路层网络拓扑发现及其 Web 表现方法[J].计算机应用, 2004, 24(7): 80 – 81, 84.
- [7] 维昭,刘强,韦卫,等.多方位网络拓扑发现的通用算法与技术实现[J].计算机应用研究, 2004, 21(12): 257 – 261.
- [8] 朱有产,李春祥.一种跨 VLAN 的网络拓扑发现算法[J].计算机工程, 2005, 31(3): 134 – 136, 139.