文章编号:1672 - 058X(2011)01 - 0059 - 04

一种基于 SNMP 的网络拓扑发现算法

郭晓永[1], 王相军[2]
(1. 临沧师范高等专科学校 数理系,云南 临沧 677000; 2. 河南检察职业学院 基础部,郑州 451195)

摘 要:网络拓扑发现是网络管理中一项非常重要的技术;网络拓扑发现的算法和实现技术是衡量网络管理系统性能的一个重要方面,基于 SNMP 的网络拓扑发现技术速度最快,使用范围也最广泛,网络层的拓扑发现算法有效地解决了路由器的多 IP 地址问题;在此研究多层网络拓扑自动发现,提出了一种基于 SNMP 协议的全新的网络拓扑发现的实现算法,使得算法更简单、效率更高。

关键词:网络管理协议;拓扑发现;网络管理;发现算法
中图分类号:TP312 **文献标志码**: A

1 常用拓扑发现方法

网络拓扑是一种表达网络逻辑连接关系和物理连接关系的方法,通过它网络管理员可以直观地了解网络当前的运行状况,准确定位网络中的故障以进行隔离,并对整个网络中可能存在的瓶颈进行准确分析,从而有针对性地改造网络,提高网络的整体性能。网络拓扑的自动发现技术成为构建网络拓扑图的关键所在。目前拓扑发现主要采用两种方案,一是利用 SNMP[1] 实现对于路由表的被动查询;二是利用 ICMP 实现基于 ping 和 traceroute 的主动探测,在此讨论的拓扑发现算法是基于 SNMP 实现。

使用 ICMP 协议构造 3 层拓扑 TCP/IP 协议规定,当路由器接收到 TTL 字段被减为 0 的 IP 报文时,路由器从其近端端口向探测源地址返回 ICMP 超时报文。Traceroute 应用程序根据此原理来检测点到点之间的路由连接状态,并获取从探测源地址到探测目的地地址之间所有经过的路由地址序列。使用 Traceroute 技术,可以对整个网络中的地址空间进行路径探测,从而可以计算出整个网络的网络层拓扑连接关系。由于 Traceroute 每进行一次探测,实际上都向网络中发送 3 个 UDP 数据包,构造整个网络的拓扑关系会产生很大的网络开销。

2 简单网络管理协议 SNMP

SNMP (简单网络管理协议)由于其简单和易于实现的特性,已经成为网络管理领域事实上的协议标准,且目前主要的网络设备都提供对 SNMP 协议的支持,因此基于 SNMP 协议的网络层拓扑发现技术被广泛采用。它的基本思想是所有的网络设备维护一个 MIB (管理信息库)保存其所有运行进程的相关信息,并对管理工作站的查询进行响应。SNMP 协议描述了一种从 MIB 库中获取信息的方法,对设备唯一的要求是支持 SNMP 并且 MIB 中的信息足够丰富。使用 SNMP 的最大优点是信息自动随网络的状况更新,这样通过 SNMP 获取的拓扑信息总是反映网络最新的状况。

收稿日期:2010 - 04 - 20;**修回日期**:2010 - 05 - 24.
作者简介:郭晓永(1975 -),男,讲师,河南镇平人,从事智能控制研究.

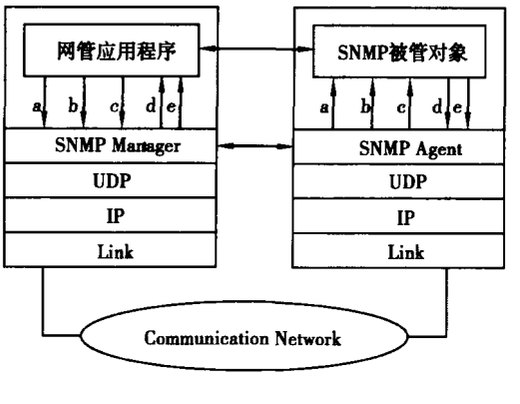
2.1 SNMP的体系结构

SNMP是以已成事实标准的TCP/IP协议为基础的。SNMP两个主要的组成部分为SNMP代理和SNMP管理者。想要监视的每个网络设备(节点)都要运行SNMP代理,SNMP代理是一个或多个软件进程,它将侦听UDP端口161上的SNMP消息并随时记录着网络设备的各种情况。网络管理程序发送到代理上的每个SNMP消息将包含有想要收集或修改管理对象的列表,用来查询或修改代理所记录的信息(图1),SNMP共提供了5种操作来完成网络的管理,Get用于获取特定的对象;Get-Next用于获取对象,但不知道其确切名称,它将允许用户遍历MIB树,并判断哪些对象存在;Set用于修改或创建对象; Get-Response回答取操作;Trap可以查找特定的事件并检测它们,发送一个Trap消息给预配置好的管理工作站。与前面几条操作不同的是Trap消息被发送到UDP端口162上。

具体地说,管理站发出Get报文,从拥有SNMP代理的网络设备中获取指定对象的信息,把所需要获取的对象标识提取到应用程序中。SNMP代理用Get-Response消息响应Get报文。Get-Next是管理站用于查询信息的报文,它可以获取一个表中指定对象的下一个对象,以遍历整个表。Get实现了对设备信息的查询,如果要求改变代理的配置,就需要管理站向被管代理发送Set报文。Set常用于对网络设备进行远程配置。SNMP陷阱(Trap)是SNMP代理发送给管理站的非请求消息,该消息通知管理站发生了特定事件。

2.2 SNMP报文格式

SNMP报文没有固定的段,而是使用标准的ASN·1编码。SNMP报文由3个主要部分组成:协议"版本"、SNMP Community(共同体名)标识符(习惯上按管理员管理网关分组)和一个"数据区域"(data area)。这个数据区域划分成若干协议数据单元(PDU:Protocol Data Unit)。每个PDU由一个"请求"(客户发送的)或一个"响应"(服务器发送的)组成,报文格式如图2所示。



a = Get;b = Get-next;c = Set;
d = Get-response;e = Trap

图1 SNMP的体系结构

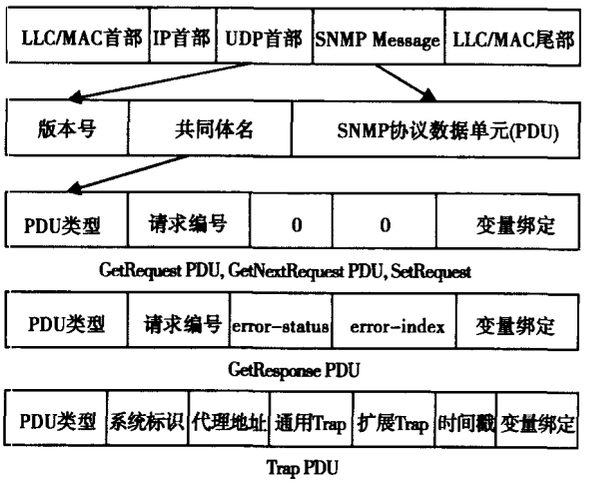


图2 SNMP消息格式

3 数据结构和算法

3.1 主要数据结构

在链路层拓扑发现中,除了使用网络层拓扑发现的部分数据结构外,还定义了如下的数据结构,同样也是使用二维链表结构来存储节点数据。

```
① struct Dot1dStpPortEntrInfo          //生成树信息
  | int dot1dStpPortState;              //端口状态
    char designaBridge[24];            //端口指定网桥
    ......
```

```
    };
② struct Dot1dTpFdbEntrInfo                    //地址转发表
    { char dot1dTpFdbAddress[18];              //MAC 地址
      int dot1dTpFdbPort;                      //对应端口索引
      int dot1dTpFdbStatus;                    //MAC 地址状态
      ......
    };
③ struct IEEE8021D                             //网桥节点
    { int dot1dStpRootCost;                    //累计根代价
      int dot1dStpRootPort;                    //根端口号
      Dot1dStpPortEntrInfo * info_stp;         //生成树信息
      Dot1dTpFdbEntrInfo * info_fdb;           //地址转发表信息
      ......
    };
```

3.2 算法实现

首先在算法中定义:outBoundAddressSets 表示与出口路由器直接相连的下一跳路由器地址集合,用它来限制网络层拓扑发现的范围,以避免因该下一跳路由器具有与被管域中设备相同的通信口令字而出现程序上扩大网络;communitySnmpReadList 表示读口令字链表对象;nexthopQueue 表示待发现的路由器地址队列;seedRouter 表示种子路由器;Gather-RouterInfoAll 函数用来收集路由器的数据,该函数返回 RouterNode 类型的节点;SnmpPing 函数使用 SNMP Get 操作原语,实现测试指定设备对某种组合方式的通信口令字、协议版本能否响应。网络层拓扑发现算法实现的流程如下:

(1) 从配置文件中读取拓扑发现配置信息,初始化如下对象:outBoundAddressSets、seedRouter、communitySnmpReadList,将 seedRouter 加入到空队列 nexthopQueue 中。

(2) 如果 nexthopQueue 为空队列,则转(7);否则取出 nexthopQueue 中队头节点,使用 communitySnmpReadList 链表作为输入,调用 SnmpPing 测试出响应的通信口令字和协议版本号。

(3) 如果(2)中没有能够找出响应的通信口令字,分两种情况处理:被测试设备地址为 seedRouter,则转(9);被测试设备地址不为 seedRouter,则转(2)。

(4) 使用(2)中测试成功的通信口令字、协议版本和设备地址作为输入参数,调用 GatherRouterInfoAll 收集路由器的地址信息 info_ipAd 和路由表信息 info_ipRo,并将返回的节点作为二维链表的纵向节点串接,同时对地址信息等链表作为横向节点进行串接。

(5) 分析(4)中收集到的节点的路由表数据。若 ipRouteType = 4,则记录该路由器与相对应的 ipRouteNextHop 值所代表的设备直接相连,同时检测该值是否存在于集合 outBoundAddressSets(避免程序上扩大网络)和横向地址信息链表 info_ipAd(解决不同地址可以代表同一个路由器的问题,避免重复访问设备)中;如果都不存在,则将它添加到 nexthopQueue 队列中。若 ipRouteType = 3,记录该路由器与子网直接相连。

(6) 重复(2)-(5)的操作。

(7) 分析横向地址信息链表 info_ipAd,找出运行 OSPF 等路由协议后因选择最短路径而可能未被记录到 MIB 中的连接关系:如果两个接口 IP 地址与对应掩码做与运算后所得的网络地址相等,它们之间是直接连接或者是同一子网间相连。

(8) 根据横向地址信息链表 info_ipAd 计算出整个被管网络中所有可能存在的主机地址集合,为链路层拓扑发现做准备。

(9) 算法结束。

4 结束语

网络拓扑发现是可视化网络管理的基础,本算法使用SNMP协议实现了网络层拓扑结构图的快速发现。但是,现在的企业内部网由于网络节点数目不多,网络流量不大,经常采用交换机完成局域网的组建,而一般的交换机工作于数据链路层,没有路由功能,所以上述方法不适合属于链路层的拓扑结构的发现。更遗憾的是上述方法只适用于同一个管理机构下的IP网络的拓扑自动发现,而对属于不同管理机构的网络(如Internet)拓扑自动发现,实现起来要复杂得多。在这两种情况下就需要采用其他技术来实现链路层网络拓扑发现和不同管理机构的网络拓扑自动发现方法,这将成为今后努力的方向。

参考文献:

[1] STALLINGS W. SNMP网络管理[M]. 胡成松,汪凯译. 北京:中国电力出版社,2001

[2] 王伟莉,陈雷. 网络拓扑发现算法的研究与实现[J]. 沈阳工业大学学报,2004,26(2):211-214

[3] MELENDEZ E, QASEM A. Methods of internet topolo-gy discovery: A compareative survey[EB/OL]. [2005-08-01]. http://www.cs.rice.edu/ qasem/papers/topology.pdf

[4] DAVID Z. 潇湘工作室 SNMPv3 与网络管理[M]. 北京:人民邮电出版社,2000

[5] 施锋,吴秋峰. 网络多层拓扑发现算法的分析[J]. 网络信息技术,2004(5):101-103

[6] DAVID G, NICK F, STEVE B. Topology inference from BGP routing dynamics [DB/OL]. http://nms.lcs.mit.edu/papers/clustering-imw.pdf

[7] 黄立慧,张春艳. 基于SNMP的网络拓扑发现算法[J]. 佳木斯大学学报:自然科学版,2008,26(4):512-514

[8] 邓泽林,张立芳,刘翌南,等. 基于SNMP协议的网络拓扑发现算法[J]. 长沙理工大学学报:自然科学版,2007,4(4):68-72

[9] 施锋,吴秋峰. 网络多层拓扑发现算法的分析[J]. 网络信息技术,2004(1):22-26

Network Topological Discovering Algorithm Based on SNMP

GUO Xiao-yong[1], WANG Xiang-jun[2]

(1. Department of Mathematics and Science, Lincang Teachers' College, Yunnan Lincang 677000, China;
2. Department of Fundamental Courses, Henan Procuratorial Professional College, Zhengzhou 451195, China)

Abstract: Network topology discovery is a key technology in network management. Algorithm and implementation of network topology discovery are important parts to evaluate performance of network management system. The SNMP-based network topology discovery has the fastest speed and is widely used. The algorithm which is suitable for network level can solve the problem of router with a few IP addresses. In this paper, we study multi-layer network topology automatic discovering, give a new protocol based on SNMP for network topology discovery algorithm for a new implementation, which causes the algorithm to be simpler, and more efficient.

Key words: SNMP; topology discovery; network management; discovery algorithm

责任编辑:代晓红