文 章 编 号: 1000-1220(2000) 08-0792-03

网络拓扑发现的主动探测技术的研究和实现

张 勇 张德运 李 钢
(西安交通大学系 西安 710049)

摘 要: 本文提出了一种有效的主动探测技术用于实现网络拓扑发现.其中利用 ICMP, DNS等协议主动收集网络的拓扑信息,并提供了通过处理信息和区分网络设备来实现拓扑生成的算法.最后利用操作系统的指纹技术实现网络系统的识别,从而形成了一套比较完整的网络拓扑发现功能.辅助网络管理人员对整个网络进行监控.

关 键 词: 拓扑发现;主动探测;指纹
分 类 号: TP393 文献标识码: A

1 引 言

随着网络规模的膨胀和复杂度的增加,网络管理在今天的网络环境中起着愈发重要的作用了.一个好的网络管理系统首先就是要掌握整个管理网络的拓扑结构.通常网络的拓扑是通过工具输入到网络管理系统中的,这对于一个规模小且变化少的网络还是可以的.但是对于一个规模较大的网络,网络的拓扑结构经常在发生一些变化.这时还采用手工的方法已经不太现实了.所以迫切需要一个方法能够自动生成网络的拓扑结构并且动态的反映网络的拓扑变化情况.本文讨论和研究了普遍实用的 IP网络拓扑发现的一些关键技术,提出了一种有效的主动探测技术来实现网络发现的方法.

2 网络拓扑发现的研究和分析

网络拓扑发现涉及到的问题比较多,但是总的来说,要对一个网络实现拓扑发现,主要有三方面问题需要明确.

(1)确定这个技术针对网络层次的哪一层及什么协议.这是因为只有确定了网络的层次和协议,才能明确到底什么样的信息要被采集,才能使这项技术具有比较好的适应性.目前随着 Internet的普及,大多数的网络都采用 TCP/IP协议,几乎所有的设备都支持 IP协议,所以这里针对 IP层相对较好.

(2)确定是采用被动监测技术还是主动探测技术来实现网络拓扑信息的采集.这两项技术相比较:

被动监测技术是通过在所有观测的网络都加入一个探测器,由它来采集信息,并发送到网络管理主机来形成网络的拓扑结构.这种技术的优点是本身除了向管理主机递交各个网络的拓扑信息,不产生额外的流量.所以产生的网络流量比较小,网络负担小.缺点是由于是各个探测器被动的通过收集各自网络中交换的信息,所以需要花费长的时间才能收集到足够的信息来形成最后的网络拓扑.并且由于要将探测器安装在所有涉及的网络中,这是对于一个大的网络来说是不太实际的.主动探测技术是通过网络管理主机主动向所有管理网络发送探测包,并采集返回的信息,进行分析最终形成网络的拓扑.这种技术的优点是:能够比较快的形成整个网络的拓扑.缺点是需要产生的流量比较大,并且对于一个十分慢的网络不太适合.

(3)确定采用何种方式收集信息.一种是采用网络管理信息协议(如 SNMP)来收集网络的信息.但是网络上的设备十分繁杂,不是所有的设备都支持这些管理协议,而且需要对涉及到的网络逐个进行配置.一种方式就是采用一种通用的协议来实现对于网络信息进行采集,这样局限性较小,如本文所介绍的方法就是基于 ICMP等协议来实现的.他们是建立在 IP层的基础上的,被所有的 IP网络和设备支持,可靠性比较高,且省去了大量的手工配置.

3 主动网络拓扑发现

本文所介绍的方法是针对 IP层,采用主动探测技术,并采用 ICMP和 DNS等协议来实现网络拓扑信息的收集,并且为了更好的实现网络拓扑的认识,还采用操作系统的指纹技术来实现对于网络中的设备进行识别,从而得到一个详细的网络拓扑结构.具体的实现步骤:

3.1 信息采集与处理

这部分包括 3部分(图 1)

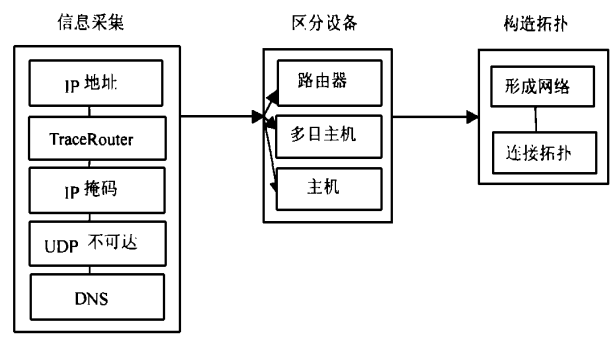

图 1

3.1.1 信息采集

(1) 确定给定地址空间的网络在线 IP地址(IP_i).这可以

收稿日期: 1999-09-24 基金项目: 国家"九五"科技攻关项目基金资助.项目编号: 96-743-01-04-01 作者简介: 张勇,博士.主要研究领域为计算机网络互连与性能管理.张德运,教授,博士生导师.主要研究领域为计算机网络互连、网络操作系统及 Cernet建设.李钢,博士生.研究方向: 网络管理信息系统. e-mail zhangy@xanet.edu.cn

通过向网络中所有可能的主机发送 ICMP响应包来实现.这里没有采用广播的 ICMP响应包,因为要避免产生广播风暴,且部分路由器等设备对这种广播具有过滤功能,导致信息的不正确.

(2)利用 Van Jacobsen算法来向所有的上面的在线 IP_i 发送路由跟踪包.并将各个设备的路由跟踪信息保存.并加入那些新的中间路由设备到在线设备地址中.如下:

$TRACE_i=(IP_1,IP_2,\ldots,IP_k,IP_i)$ 代表地址 IP_i 的路由跟踪数据.$\in$ IPADDR

IPADDR代表前一个步骤发现的所有在线 IP的地址集.

IP_i:代表 IPADDR中的第 i个 IP.

对于任意的 $TRACE_i$,如果 $IP_j\in TRACE_i$ 且 $IP_j\notin$ IPADDR,则添加 IP_j 到 IPADDR.

(3)确定所有在线设备的网络掩码($MASK_i$).这可以通过发送 ICMP mask信息来实现.

(4)向所有的在线设备的一个无用的端口发送 UDP包,并存储返回的 IP地址(FIP_i)

(5)确定所有在线设备域名(DNS_i).通过发送 DNS包.

现在通过上面五个步骤就实现了网络拓扑信息的采集.然后就是如何来识别网络的设备和形成最终的网络拓扑了.

3.1.2 区分设备

一个 IP网络中的设备关键有三类:路由器、主机、多目主机.首先就是要区分出这些设备.分三步骤完成:

(1)路由器 根据 Trace Router的特点,除了路由跟踪 IP的最后一个为目标地址,其余 IP地址的都是路由设备.所以首先标明这些 IP地址对应的为路由器.但是路由器通常有多个接口地址,根据这项信息并不能确定其他几个接口的地址.但是根据 trace路径的下一个 IP地址和 MASK地址可以得到其他的端口地址.如下:

对于任意的 $TRACE_i=\{IP_h,\ldots,IP_{i-1},IP_i,IP_{i+1}\ldots IP_j,IP_i\}$

如果 $IP_i\in TRACE_i$,且 $IP_j\neq IP_i$且 $IP_j\notin$ ROUTER,则添加 IP_j到 ROUTER.

根据 IP_{i+1},$MASK_{i+1}$,可以得到路由器 $ROUTE_i$ 这个接口的所接的网络 NET_i

对于任意的 $IP_m\notin NET_i$,判断 $TRACE_m=TRACE_i$,则 IP_m为路由器 $ROUTE_i$ 的一个接口.将其从 IPADDR中提出.并加入到 $ROUTE_i$.

(2)多目主机 这类主机具有不止一个 IP地址,所以应该将同一多目主机的地址合并起来.这可以通过 DNS和 FIP实现.如下:

对于任意的 IP_i,如果 $IP\neq FIP_i$,则可以将 FIP_i 加入到 $MULTIIP_i$

判断 $IP_{ID(FIPi)}\neq FIP_i$,则将 $IP_{ID(FIPi)}$加入到 $MUTLTIIP_i$,

如此下去直到 $IP_{ID(FIPi)}=FIP_i$,

然后将所有的 $IP_i\notin MULTIFIP_i$,从 IPADDDR中提出.

然后判断任意两个 DNS_i,$DNS_k\neq$ 空,对应的 IP为 IP_i和 IP_k,且 IP_i,$IP_k\notin$ ROUTER 如果 $DNS=DNS_k$,且

a. IP_i和 $IP_k\notin MULTIIP$,则生成 $MULTIIP_i$.

将 IP_i和 IP_k加入到 $MULTIIP_i$,并从 IPADDR中提出 IP_i,IP_k

b. $IP_i\notin MULTIIP$,$IP_k\in MULTIIP_K$,则将 IP_i加入到 $MULTIIP$,并从 IPADDR中 提出 IP_i

c. $IP_k\notin MULTIIP$,$IP_i\in MULTIIP_i$,则将 IP_k加入到 $MULTIIP$,并从 IPADDR中 提出 IP_k

(3)主机:这些是除了路由器和多目主机之外的网络设备.每个主机具有单独的 IP地址.现在经上面两步.剩下的 $IP\in$ IPADDR,就都为主机.

3.1.3 形成拓扑

经过上面三个处理过程就区分出了网络中的主要的三类设备.现在就是通过这些设备的特点容易形成网络的拓扑.

(1)区分网络.根据网络中的路由器接口地址和网络掩码,可以得到这个路由器所连接的网络地址 NET_i 及其范围.从而可以得到所有的网络.

(2)连接网络和主机,形成最终的拓扑图.首先连接各个路由器和所连接的网络,这由上一步可以得到.

然后连接主机和对应的网络,这里不采用主机地址 IP_i 和网络 $MASK_i$,因为主机的 $MASK_i$ 不可靠.可以根据路由跟踪 $TRACE_i$ 得到每个主机所连接的路由器,并由此可以得到对应的网络.并连接这个主机和对应的网络.如图 2所示.

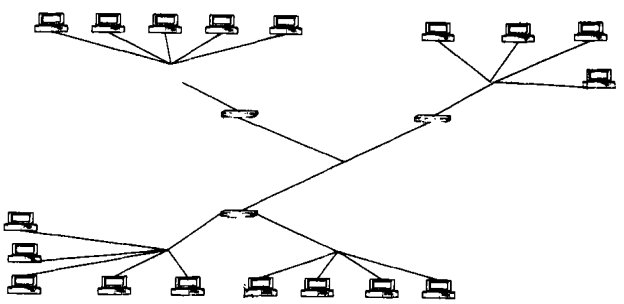

图 2

3.2 系统的识别

上面已经将网络的基本拓扑构造出来了,但是设备的分类比较简单.不能详细的知道各个设备的系统.所以最好能够将各个设备的系统区分出来.如主机采用的操作系统和路由设备的类型等,这样就能给于网络管理人员更加全面的网络整体结构的认识.如何来实现这一步呢?

经过分析和研究,不同的网络操作系统在处理网络信息时是不完全相同的,存在着各自的特点.这些特点就称为系统的"指纹".通过识别这些指纹就可以实现网络系统的识别.下面的一些方法综合起来就可以识别一个系统.如下:

1. FIN 探测:通过向系统的一个开放的端口发送 FIN包.按照 RFC793系统不返回响应.但是一些系统如 MS Windows, BSDI, CISCO, HP/UX, MVS,和 IRIX 都会返回一个 RESET.

2. TCP ISN 采样:系统在实现 TCP时,对一个连接请求的响应包的初始序列号是不同的.

是否设置分段位: 许多操作系统开始设置不分段位,从而增进系统的一些性能.

3. TCP初始窗口大小: 有些系统的初始 TCP窗口大小是独特的.如: AIX是 0x3F25.

4. ACK值: 许多操作系统的 ACK值是不标准的.

5. ICMP出错信息的频率: 一些操作系统按照 RFC1812,限制了出错 ICMP包的发送频率.

6. ICMP出错信息的形式: 许多操作系统在处理 ICMP出错信息是不是按照标准格式,导致返回的信息存在着略微的不同.

7. TOS: 有些系统在返回 ICMP端口不可达信息时, TOS值不为 0.

8. 分段的处理: 一些系统在处理重复的 IP分段信息时是不同的.

9. TCP选项: 不同的操作系统对于 TCP选项的支持是不同的.有的多些,有的少些.且在处理返回时存在着格式和顺序的不同.这些可以很好的用于识别系统.

10. SYN洪泛: 一些操作系统当接收较多的孤立 SYN包,会停止接收新的连接.从而保证系统的稳定.所以可以发送一定数量(典型 8个)的 SYN包来根据系统的处理方式区别系统.

只采用其中一种方法往往是不足于识别系统,但是将他们组合起来就能够形成一个识别系统的"指纹".例如识别一个路由器是否是 CISCO2511系列的.可以判断如下的"指纹"特征:

(1) 判断 TCP ISN是否是随机增加的

(2) 发送一个带有 TCP选项的 SYN包到一个开放的端口.判断收到的响应包中: 不分段位设定;窗口的设定为 860;响应的初始序列号为初始序列号+ 1.而且 ACT和 SYN标志在响应中发送过来.响应中的选项 MSS为被设定.

(3) 发送一个带有 TCP选项的 NULL包到一个开放的端口.判断: 一定有响应包返回;不分段位设定;窗口的设定为 0;响应的初始序列号为初始序列号.而且 ACT和 RST标志在响应中发送过来.响应中的选项设定空.

(4) 发送一个带有 TCP选项的 SYN| FIN| URG| PSH包到一个开放的端口.判断: 一定有响应包;不分段位设定;窗口的设定为 860.响应的初始序列号为初始序列号+ 1.而且 ACT和 SYN标志在响应中发送过来.响应中的选项 MSS为被设定.

(5) 发送一个带有 TCP选项的 ACK包到一个开放的端口,判断响应包中: 不分段位设定,窗口的设定为 0;响应的初始序列号不固定.而且 ACT标志在响应中发送过来.响应中的选项设定空.

(6) 发送一个带有 TCP选项的 SYN包到一个关闭的端口.判断响应包中: 不分段位设定;窗口的设定为 0;响应的初始序列号为初始序列号+ 1.而且 ACT和 RST标志在响应中发送过来.响应中的选项设定空.

(7) 发送一个带有 TCP选项的 ACK包到一个关闭的端口.判断响应包中: 不分段位设定;窗口的设定为 0;响应的初始序列号为不固定.而且 RST标志在响应中发送过来.响应中的选项设定空.

(8) 发送一个带有 TCP选项的 FIN| PSH| URG包到一个关闭的端口.判断: 一定有响应包;不分段位设定;窗口的设定为 0;响应的初始序列号为初始序列号.而且 ACT和 RST标志在响应中发送过来.响应中的选项设定空.

(9) 发送一个 UDP包到一个关闭的端口.判断: 没有响应包.如果上面的所有测试都通过就可以确定这台路由器是一个 CISCO 2511路由器.

4 结 论

网络拓扑发现技术是一项很有实用价值的技术,方便了网络系统的维护和管理,成为现有网络管理系统的一个很好的补充.其中本文提出的进行动态探测技术和系统识别的方法,具有较强的实用性.但是这项技术也存在着一定的缺点.就是要求网络中不存在路由循环且由于采用主动发送技术,所以对于网络的负担比通常的被动监测技术要大,但是通过和被动监测技术结合起来就能够很好的实现一个网络拓扑的动态观察效果.识别技术则由于操作系统的不断改进,版本的更新."指纹"在不断变化,所以需要不断的进行更新.目前这项技术已经应用到了实际中了.

参 考 文 献

1 J. Case, K. McCloghrie, M. Rose, S. Wald-busser. Introduction to version 2 of the Internet-standard Network Management Frame-work. RFC 1441, April 1993

2 D. C. M. Wood, S. S. Coleman, and M. F. Schwartz. Fremont: a system for discovering network characteristics and problems. [C] Proc. USENIX Winter Conference, 335~ 347, January 1993

3 J. Postel. Internet control message protocol. RFC 792, September 1981

RESEARCH AND IMPLEMENTATION OF NETWORK TOPOLOGY DISCOVERING BASED ON ACTIVE PROBING TECHNIQUE

ZHANG Yong ZHANG De-yun LI Gang
(*Xi an Jiaotong Universiy network institute Xi an* 710049)

Abstract This paper presents a efficient active probing technique to discover the network topology. The discovering mechanism actively probe the network to gather information using ICMP and DNS packets. And the paper provide a good algorithm to handle the information and distinguish the network device. It uses the fingerprinting of network OS to identify the network device in detail. So it implements a set of integrated methods to dicover network topology and help network managor to monitor the network.

Key words Topology discovering; Active probing; Fingerprinting