基于拓扑发现的设备监控系统

肖通[1]，龚俭[1]

（1.东南大学网络空间安全学院，南京，210000）

摘　要：本文以华东北地区网络中心的网络环境为背景，基于 SNMP 协议，利用多线程并发算法实现拓扑发现系统，并基于拓扑发现系统的实时数据，实现对接入设备的监控。通过该系统，能够实现对网络设备的探测，并且发现速度时间大大降低，具有较好的实时性。

关键词：拓扑发现；设备监控；SNMP 协议

Device monitoring system based on Topology Discovery

Xiao Tong[1], Gong Jian[1]

(1. School of Cyber Science and Engineering, Southeast University, Nanjing, 210000)

Abstract: In this paper, the network environment of Northeast China Network Center is taken as the background, based on SNMP protocol, the topology discovery system is realized by using multithread concurrent algorithm, and the access equipment is monitored based on the real-time data of the topology discovery system. Through this system, the detection of network equipment can be realized, and the speed time is greatly reduced, which has better real-time performance.

Key words: Topology discovery; Device monitor; SNMP

1 引言

网络管理是指监督、组织和控制网络通信服务以及信息处理所必须的各种活动[1]。网络管理是为了保障计算机网络持续、平稳、正常的运行，并且当计算机网络运行出现异常情况时，能够及时响应和排除故障。

在网络管理系统中，为了能够通过一种直观、有效的方式,将当前的网络信息呈现给网络管理者，需要能够让网络管理者实时地看当前的网络拓扑连接情况。网络拓扑图能够显示当前网络中存在的设备节点信息和设备节点信息之间的连接关系[2]，从而对当前网络的网络连接进行及时地反映，对网络环境实时准确地监控，掌握网络态势，及时发现设备的异常情况和网络的故障及异常行为。

本文围绕 CERNET（China Education and Research Network，中国教育科研网）华东北地区网络中心的实际情况，使用拓扑发现技术对相关问题的解决方案进行探索。

目前，华东北地区网络中心供了有线接入和通过无线网络接入两种方式，为网络中心的师生提供了科研和学习的网络服务，增加了用户的便利性的同时，也使得网络中心的内部网络环境日益复杂。目前网络中心内部接入的设备多达数百台，且类型多样，包括交换机、PC 机、AP（Access Point，接入点设备）设备以及移动终端（手机、平板）等。因此，需要对内部网络中所接入的设备进行监控。为了使网络管理人员能够对接入设备进行有效管理，时发现和响应网络中的异常情况，开发针对性的网络管理功能是十分必要的。

基于上述分析，为了实现设备监控的目标和要求，需要该系统能够满足以下三点需求：第一，完整性，也就是能够对当前网络环境中的所有设备进行发现和监控，从而能够全面完整的反应网络中设备的情况；第二，实时性，也就是要求系统能够及时快速的反应当下网络环境中网络设备的接入情况和连接情况，从而能够对设备做到实时的监控；第三，高效性，也就是要求系统在进行设备监控时，能够快速高效的进行设备的探测，进一步也保证了系统的实时性。

作者简介：肖通，（1995-），男，硕士研究生，E-mail: txiao@njnet.edu.cn；龚俭，（1957-），男，教授，E-mail: jgong@njnet.edu.cn.

基于上述研究背景和现状，本文对现有的内网的网络管理系统进行了改进，使用拓扑发现技术，并且基于多线程并发算法，做到对网络内接入的设备实时快速的发现，并进一步进行监控。

2 相关技术

2.1 拓扑发现技术

拓扑发现[3]是指利用技术手段来发现整个网络中存在的设备节点信息以及设备节点之间的连接关系。其目的是探究网络中设备的拓扑结构信息，并描述设备之间的互联关系，最终形成网络拓扑图。通过网络拓扑图，网络管理人员能够了解网络环境之中的设备连接情况，并且通过了解网络环境的拓扑结构，对网络中的设备进行管理、诊断、配置、优化和监控。

网络拓扑发现可以分为两个过程[4]，包括探测和分析。探测阶段采取技术手段来获取拓扑的数据信息，分析阶段则是在探测阶段获取到的数据的基础之上进行分析研究，获取设备之间的关系，最终生成拓扑图。整个过程也就是使用探测主机运行拓扑发现程序，进一步地向被管网络发送报文，然后获取回应，进行分析，然后提取网络拓扑信息，生成该网络的拓扑结构。

为了实现拓扑发现，常用的方法有几种：基于SNMP（Simple Network Management Protocol，简单网络管理协议）协议的拓扑发现方法；基于 ICMP（Internet Control Message Protocol，网络控制报文协议）协议的拓扑发现方法；基于路由协议的拓扑发现方法；基于 DNS 协议的拓扑发现方法等。表 1 对几种拓扑发现方法进行了对比。

表 1 拓扑发现方法对比表

对比项	SNMP	ICMP	路由协议	DNS
速度	中	慢	快	中
精度	高	低	低	中
负载	高	高	低	低
实现难度	易	中	难	中
应用范围	大	小	小	中

基于上述比较，本文采用基于 SNMP 协议的方法进行拓扑发现。

2.2 SNMP 协议分析

SNMP 即简单网络管理协议，是 Internet 标准网络管理框架[5]。SNMP 使用“管理——代理进程模型”，在管理站和代理站之间通过 SNMP 协议来传递消息[6]。SNMP 协议是一个应用层协议，基于 UDP 协议，使用 161 端口。

MIB（Management Information Base）即管理信息库，是代理进程包含的能够被管理进程查询和设置的信息的集合，是一个虚拟的信息存储器[7]，包含了全部被管理对象的相关信息。被 SNMP 管理的每台主机上都包含一个 MIB，这个 MIB 描述了该主机上的可管理对象。MIB 中的信息使用 SMI 进行定义。SMI（Structure of Management Information）即管理信息结构，使用 ASN.1（抽象语法记法 1）来定义数据类型。OID（Object Identifier）即对象标识符是 ASN.1 的一种数据类型，标识了有唯一性标识的信息性实体。对象标识符是一个整数序列，由（“.”）进行分割。所有的对象标识构成一个类似 DNS 的树形结构。

一般情况下，使用 MIB-II 节点组也即 1.3.6.1.2.1 起始的 OID 来实现网络管理。主要使用的信息包括：System 组：提供被管系统相关信息；Interfaces 组：提供网络接口相关信息；TCP 组：提供设备与 TCP 相关的数据信息；IP 组：提供设备与 IP 相关的数据信息。

SNMP 协议定义了五种操作，分别为：Get-Request: 查询请求，由管理站发出 get-request 请求，请求中包含了请求编号 request-id 以及被请求对象的实例列表。代理进程收到请求后，返回 get-response 进行应答；Get-Next-Request: 查询请求，由管理站发出该请求，请求中包含内容与 get-request 相同。代理进程收到请求后，返回 get-response 进行应答。查询的是请求对象的下一个对象；Set-Request: 设置请求，管理站发出，报文中包含了设置的对象和参数，代理进程收到请求后进行处理，然后返回 get-response 进行应答；Get-Response: 应答，由代理进程向管理进程发出，是向管理进程的查询以及设置报文的回应，包含了处理的结果和错误信息；Trap: 代理进程主动发出，用来通知管理进程本设备有关事件的发生。

3 系统设计

网络中心中拥有多台交换机及PC设备组成的有线网络，以及由 AC（Access Controller，接入控制器）及多个 AP 构成的 WLAN 无线网络。基于上述背景，本文采用基于SNMP协议的拓扑发现技术，进行网络接入设备的实时探测，进一步生成网络拓扑图，并基于实时发现的拓扑发现数据进行设备的监控。系统整体的设计思路，如下图所示：

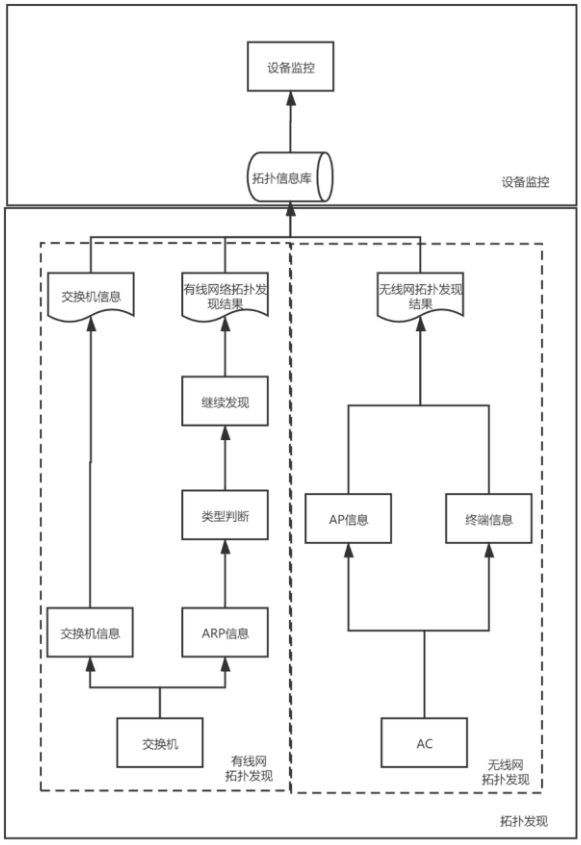

图 1 设备监控系统设计图

在有线网拓扑发现中，首先通过 SNMP 协议获取交换机相关信息，包括交换机自身的相关参数，以及 ARP 表数据，分别用来进行交换机监测以及进一步的拓扑发现。在获取到 ARP 表数据后，对其中包含的设备进行设备类型的判断，从而进一步的进行拓扑发现，直到得到完整的探测结果。在拓扑发现的过程中，保存设备之间的连接关系的数据信息，最后统一进行处理，得到最终的有线网络拓扑关系，保存到拓扑信息数据库中。

在对 WLAN 的拓扑发现中，由于 AP 为瘦 AP，并不支持 SNMP 协议，但是 AP 相关信息注册到 AC 设备之上，因此，需要通过 SNMP 协议采集 AC 设备上的 AP 的相关数据，最终得到 WLAN 网络的拓扑。首先，采集 AC 设备上的有关 AP 的数据，以及接入 WLAN 的终端设备的数据；然后通过对这两部分数据进行处理，最终得到 AP 及对应终端的对应关系，也就得到了最终的无线网络拓扑发现结果，保存到拓扑信息数据库之中。

通过拓扑发现得到的结果，保存到拓扑信息数据库之中。基于拓扑信息数据库的结果，构建内网的设备拓扑图，以供网络管理员进行查看。同时设置设备监控模块，对所需要监测的设备，针对拓扑信息数据库的最新结果，从而及时发现设备的相关异常情况。

4 系统实现

4.1 有线网络拓扑发现

对有线网络进行拓扑发现，主要是需要探测设备之间的互联关系，由于目前网络中心的设备都支持 SNMP 协议，因此使用 SNMP 协议结合 ARP 协议来进行拓扑发现。整个有线网络拓扑发现的过程如图 2 所示，包括如下步骤：

1. 以内网顶层交换机为起点，使用 SNMP 协议采集交换机的相关信息；

2. 根据交换机的 ARP 表，获取交换机接口上连接的设备信息，主要是 MAC 地址和 IP 地址；

3. 对新发现的 IP 地址通过 SNMP 协议采集设备信息，判断设备的接口个数，进一步判断设备的类型；

4. 将判断为是主机的设备与交换机连接关系进行存储；

5. 将判断为交换机的设备加入到队列中，重复步骤 3；

6. 当交换机队列为空时，拓扑发现结束。

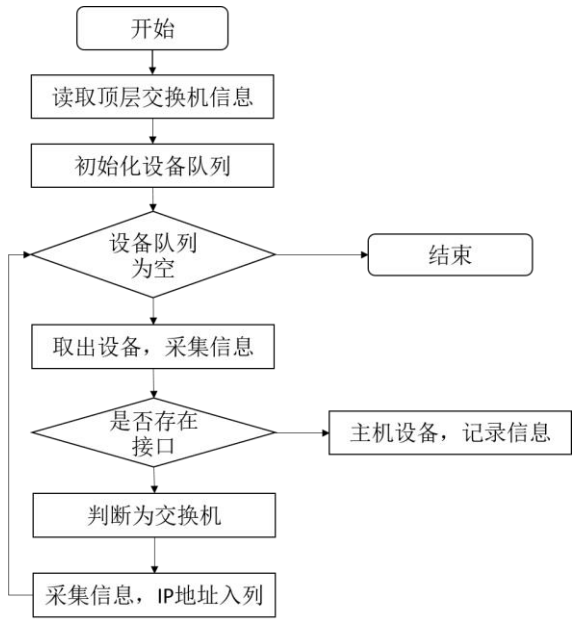

图 2 有线网络拓扑发现流程图

图 2 介绍了拓扑发现算法的整体流程，获取和更新网络拓扑信息需要周期性的扫描 SNMP 信息。有实验表明，在网络规模较大，结构复杂的网络中，拓扑发现的大部分时间消耗都来自请求数据的阶段[8]。由于 SNMP 信息的获取需要耗费大量的时间，且主要的时间消耗在网络数据的请求之上。因此，要提高拓扑发现系统的性能，加快一次完整拓扑发现的速度，就需要提高数据的获取效率。基于如上分析，本文提出了基于多线程的并发拓扑发现算法，通过并行扫描设备，充分利用系统的资源，且相比多进程更加灵活方便，占用系统资源更少。因此，采用异步多线程的方法进行拓扑发现，对多线程采用线程池进行管理。

基于并发算法的拓扑发现执行过程如图 3 所示：

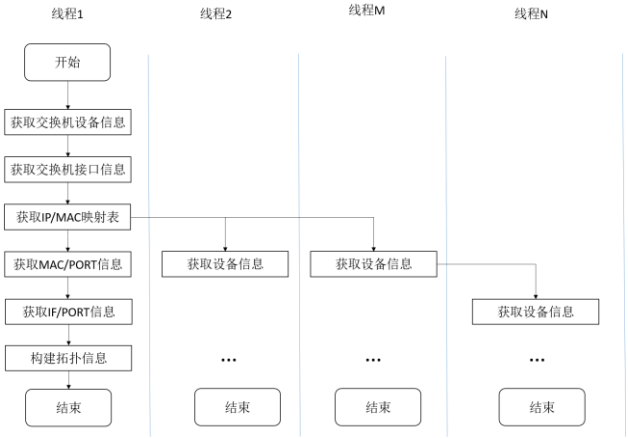

图 3 并发拓扑发现算法执行过程

算法采用了并发编程的方法，使用线程池进行实现。在线程池中，维护 N 个线程，线程用来执行提交的任务。在算法中，提交的任务是指，对指定的 IP 地址进行 SNMP 信息的采集。当任务提交到线程池时，首先会判断当前线程池的线程数量，如果未达到最大线程数 N，则线程池会创建一个新的线程来执行所提交的任务；如果达到最大线程数 N，则线程池会判断是否有空闲的线程，有则将任务交给空闲线程来执行；如果达到最大线程数 N，且没有空闲的线程，则会等待线程空闲，直到有空闲线程可以执行任务，则提交给该线程。

针对每个任务而言，具体的执行过程如下：

1. 获取设备的端口数，从而判断设备是主机还是交换机；

2. 如果是主机，任务结束。

3. 如果是交换机，首先采集 system 组中交换机的相关信息，保存到数据库中；

4. 进一步采集交换机的接口信息，保存到交换机相关的表中；

5. 采集交换机的 IP/MAC 地址信息，此时根据 IP 集合创建新线程，新线程去执行步骤 1），并将该信息暂时保存；

6. 采集交换机的 MAC/PORT 信息，从而得到<IP,MAC,PORT>的三元组；

7. 采集交换机的 IF/PORT 信息，从而将步骤 6 中的<IP,MAC,PORT>的三元组替换为<IP,MAC,IF>的三元组，也就是得到了交换机各个接口下联设备的 IP 和 MAC 地址信息。到此，该任务执行结束。

4.2 无线网络拓扑发现

在本文中，针对网络中心的 WLAN 进行拓扑发现，使用的 WLAN 网络设备主要是 AC 和瘦 AP。

瘦 AP 与胖 AP 不同，胖 AP 主要应用于小型无线局域网之中，集物理层、用户数据加密、认证、QoS、网络管理等功能与一身。而瘦 AP 一般需要和 AC 配合使用，其中 AC 集中处理与安全、管理以及控制相关的功能，而瘦 AP 只负责提供可靠和高性能的无线射频功能。这种组合的方式中，AC 负责管理 AP 资源，瘦 AP 提供有限的功能，因此不能与管理系统进行直接的交互，需要通过与之关联的 AC 设备来获取相关的管理信息。

与上一小节中有线网络拓扑发现类似，本文仍采用基于 SNMP 协议的方式采集 AC 的相关信息，

进一步获取 AP 以及接入终端的信息，最终得到完整的网络拓扑。

算法实现流程如图 4 所示，包括如下步骤：

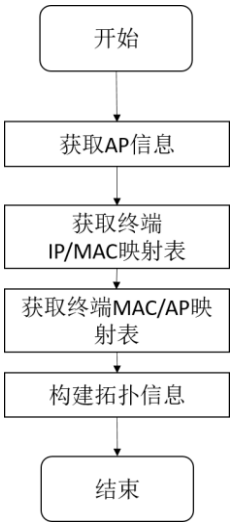

图 4 无线网拓扑发现算法

1. 采集 AP 相关信息，得到 AP 的<IP, MAC, 序列号>信息，根据该信息更新 AP 的配置信息以及 AP 的相关性能数据；

2. 采集接入该 WLAN 的所有终端的 IP 地址和 MAC 地址的对应关系信息；

3. 采集终端的 MAC 地址和 AP 的序列号的对应关系信息；

4. 根据上述三个步骤获取到的对应关系表，最终组合出<终端 IP 地址，终端 MAC 地址，AP>三元组，得到最终的无线网拓扑关系。从而完成一次无线网拓扑发现过程。

4.3 数据存储与更新

经过有线网络拓扑发现和无线网络拓扑发现，获得了最新的拓扑信息，保存在拓扑信息数据库中。数据库包含交换机信息表、主机信息表、AP 信息表以及移动终端信息表。前两个表用来存储有线网络拓扑发现中获取的交换机和主机信息，后两个用来存储无线网络拓扑发现中获取的 AP 信息以及接入无线网络的移动终端信息。

由于要求拓扑发现的结果应该具有实时性，因此，需要周期性运行拓扑发现算法，然后根据每次拓扑发现算法得到的结果，对数据进行更新。在每一次拓扑发现算法运行结束后，根据本次拓扑发现算法的结果，对数据库信息进行更新。由于交换机和 AP 信息较少，且较为固定，因此更新时会根据最新一次拓扑发现的结果直接修改相关信息，对于主机信息，更新的规则如下：

1. 对于扫描到的表格中未出现的设备 MAC 地址，说明该设备首次出现，将该设备的信息直接插入到数据库之中；

2. 对于已经出现过的 MAC 地址，比对该 MAC 地址所出现在的交换机和接口信息，如果和该 MAC 地址在表格中最后一次存储的信息不一致，说明该 MAC 地址的拓扑信息发生了改变，则将新的信息插入到数据库之中，否则进入 3）；

3. 如果该 MAC 地址与表格中存储的拓扑信息一致，说明信息没有发生变化，则更新该 MAC 地址的最后一次扫描时间。这样的规则同样适用于移动终端信息的更新。

5 系统测试

为了验证本章的设计与实现，本文基于网络中心的实际网络环境，对网络进行基于 SNMP 协议的拓扑发现，构建内网的网络拓扑图，并对设备进行相应的管理。本节首先对有限网络拓扑发现功能、无线网络拓扑发现功能进行测试，验证其功能实现。然后对拓扑图功能和设备监控功能进行测试，这两个功能都是基于拓扑发现采集到的信息进行处理实现的。最后，对拓扑发现的程序进行性能测试。

在拓扑发现时，会采集接入的主机的状态。测试时以某一服务器为例，可以看到主机首次探测到的时间，以及主机最近一次被探测到的时间，以及主机所接入的交换机和端口。此时主机在运行状态，说明系统成功发现了主机的接入信息。

图 5 主机接入状态图

拓扑发现还能够发现各个 AP 下所接入的设备信息。首先，查看当前 AP 所接入的设备信息，如图 6 所示。然后，使用手机接入该 AP，可以看到 AP 接入的设备增加了一条，并且该设备的 MAC 地址出现在了 AP 的接入设备列表之中，如图 7 所示。两张图的对比说明，该系统成功的探测到移动终端接入的信息。

ip地址	mac地址	连接AP的IP地址
211.65.196.13	90:78:41:42:fa:09	1.1.1.35
211.65.196.26	00:cd:fe:5a:ab:fa	1.1.1.35
211.65.196.36	60:14:b3:ad:cf:f5	1.1.1.35
211.65.196.38	34:e1:2d:78:5b:31	1.1.1.35
211.65.196.45	24:fd:52:b4:37:35	1.1.1.35
211.65.196.50	c0:b8:83:da:5f:57	1.1.1.35
211.65.196.64	d4:6d:6d:62:f3:fe	1.1.1.35
211.65.196.98	5c:ad:cf:57:18:5e	1.1.1.35

Showing 1 to 8 of 8 entries

图 6 接入 AP 设备信息图

ip地址	mac地址	连接AP的IP地址
211.65.196.13	90:78:41:42:fa:09	1.1.1.35
211.65.196.26	00:cd:fe:5a:ab:fa	1.1.1.35
211.65.196.36	60:14:b3:ad:cf:f5	1.1.1.35
211.65.196.38	34:e1:2d:78:5b:31	1.1.1.35
211.65.196.45	24:fd:52:b4:37:35	1.1.1.35
211.65.196.50	c0:b8:83:da:5f:57	1.1.1.35
211.65.196.64	d4:6d:6d:62:f3:fe	1.1.1.35
211.65.196.70	9c:2e:a1:eb:2d:f5	1.1.1.35
211.65.196.98	5c:ad:cf:57:18:5e	1.1.1.35

howing 1 to 9 of 9 entries

图 7 终端接入 AP 后设备列表

为了验证多线程并发拓扑发现算法程序的耗时情况，本文首先使用单线程进行一次拓扑发现，然后使用多线程并发算法运行四次，进行拓扑发现。得到的结果如下表所示：

表 2 性能测试表

测试名称	耗时
串行扫描	105.368 秒
并行扫描 1	42.206 秒
并行扫描 2	38.421 秒
并行扫描 3	34.956 秒
并行扫描 4	36.973 秒

从表 2 中可以看出，并行扫描运行一次的速度要远胜于串行扫描，说明多线程并发扫描算法能够最大限度的利用服务器资源，减少了 SNMP 请求所需要的等待时间，进而提高了系统的响应效率。此外，并发拓扑发现算法四次运行的平均时间为 38.139 秒，因此该算法进行一次完整的网络拓扑发现，需要大约 38 秒的时间，包括了若干台网络设备，包括交换机、AC 和 AP 设备，以及约 300 台主机设备，约 100 台无线终端设备。

6 总结

本文结合 CERNET 华东北地区网络中心的实际网络环境，针对网络管理需求，参考经典的 SNMP 协议算法，提出了基于多线程并发算法的拓扑发现系统，能够对网络中心内接入的设备进行实时、完整的探测，并基于拓扑发现的结果对设备进行监控。

参考文献

[1] 刘艳超, 纪妙. 基于 SNMP 的统一网管框架的设计与实现[J]. 中国新通信, 2019.

[2] 欧珊珊. 基于 SNMP 的通信网络管理系统的设计[J]. 信息通信, 2019.

[3] 肖坤峨. 简单网络管理协议 SNMP 的研究及应用[J]. 信息与电脑(理论版), 2018.

[4] 吴金晓. 基于 Cacti 的集成网络运行管理平台的设计与实现[D]. 南京: 东南大学, 2016.

[5] 尤澜涛, 朱巧明, 李培峰. 一种快速网络拓扑发现算法的设计与实现[J]. 计算机应用与软件, 2007, 24(9): 181-183.

[6] Wikipedia. SNMP Version3[EB/OL]. http://en.wikipedia.org/wiki/SNMP#Version_3, 2011-09-21.

[7] 谢希仁. 计算机网络[M]. 第七版. 北京: 电子工业出版社, 2017.

[8] 屈立成. 基于多线程扫描的网络拓扑边界监测系统设计[J]. 中国电子网, 2018.