

# 网络拓扑多端扫描机制的研究

柴艳娜<sup>1</sup>, 李 佳<sup>2</sup>

(1. 长安大学 教育技术与网络中心, 陕西 西安 710064;  
2. 长安大学 信息工程学院, 陕西 西安 710064)

**摘 要:**网络拓扑的获取是网络管理的一个重要任务。传统的网络拓扑扫描无法实现拓扑的增量扫描,不能及时更新拓扑和响应管理者的操作。为了更实时快速地反映拓扑信息及其变化,文中提出了网络拓扑多端扫描的遍历机制,利用并行高效的网络多端遍历模型,通过 SNMP 收集网络的路由等状态信息,检测并控制节点的状态属性,采集准确的网络拓扑并存储。同时针对网络拓扑实时变化追踪对网络管理的即时要求,提出了网络拓扑档案的概念,并针对拓扑档案的更新、比对与输出等问题进行讨论。

**关键词:**多端扫描;数据组织与分发;拓扑档案

中图分类号:TP39

文献标识码:A

文章编号:1673-629X(2013)09-0215-04

doi:10.3969/j.issn.1673-629X.2013.09.054

## Research on Multiterminal Scanning Mechanism of Network Topology

CHAI Yan-na<sup>1</sup>, LI Jia<sup>2</sup>

(1. Education Technology and Network Center, Chang'an University, Xi'an 710064, China;  
2. College of Information Engineering, Chang'an University, Xi'an 710064, China)

**Abstract:** Acquiring network topology is an important task of the network management. The traditional network topology scanning can't achieve the increment scanning of the topology, can't update topology and response management operation timely. In order to reflect the real time information of topology and its alteration quickly, put forward a multiterminal scanning mechanism of the network topology, with the use of parallel and efficient multiterminal traversal model, collect routing state information of network via SNMP to detect and control the property of the nodes, get accurate network topology and keep stored. Meanwhile, due to the immediate requirements of network management for real-time changes tracking in network topology, the concept of the network topology archives is proposed, discussing about the updating, comparison and output of the topology archives as well.

**Key words:** multiterminal scanning; data organization and distribution; topology archives

## 0 引言

网络的建设、维护、优化、监测以及安全等各种管理活动都是以网络拓扑为基础,因此,获得一份准确、详实、全面的网络拓扑便是网络管理的首要任务<sup>[1]</sup>。

获取网络拓扑便要网络进行遍历扫描<sup>[2]</sup>。传统网络遍历模型是以 BFS 算法或 DFS 算法为模型,网络中某个路由器为扫描起点进行遍历<sup>[3]</sup>。从起点开始扫描,逐步获取路由信息,继而遍及整个网络。当整个网络遍历扫描完成后,网络拓扑便被获取。

传统扫描模型中,整个扫描是一个从起始节点到达最后一个节点的完备唯一的过程<sup>[4]</sup>。传统模型一般的具体实现都是在一个进程/线程中实现逻辑与控制。

同时,传统模型的扫描路径与所采用的算法有关,且扫描过程的连贯性和扫描路径与逻辑连接的无关性,导致其无法实现增量扫描,在局部扫描与更新信息上显得被动,无法及时增量更新拓扑和响应用户的操作。为了更实时快速地反映拓扑信息及其变化,文中提出了多端扫描的遍历模型。

## 1 网络拓扑的多端扫描模型

### 1.1 多端扫描模型

多端遍历性扫描模型将完整的扫描过程分解成  $n$  个简单快速的子过程,每个子过程就是一次细微的扫描 (Tiny Scan, TS),只不过子过程的扫描只是扫描获

收稿日期:2012-11-26

修回日期:2013-03-02

网络出版时间:2013-05-09

基金项目:陕西省信息化重点建设项目(2171-20120042)

作者简介:柴艳娜(1984-),女,硕士,助理工程师,研究方向为计算机网络应用与信息技术。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20130509.1058.022.html>

取该节点的邻接信息从而发现后续节点,但不会外延去扫描这些邻接节点。多端扫描模型并不以唯一的起始节点为起点,而是每个节点都是某个子过程的起点,当子过程扫描完该节点,获得邻接信息后,此子过程便结束任务而消亡,它在结束前根据邻接信息重新并发产生多个子过程。

当一个子扫描过程 TS 结束的时候,又会根据其所得到的邻接信息对每个节点生成并发执行的 TS。相比起传统模型中的扫描,TS 是完整扫描的高粒度化,因而能够更加灵活、更加方便地进行扫描。

对于任意的扫描模型,网络的规模大小对所使用的扫描时间都会有直接的重大影响,同时,在遍历扫描的过程中,系统不可避免地要进行大量的收发报文操作,将会对网络设备的运行造成一定程度的影响。在设计的过程中,需要设计相对合理的设备轮询方式和方法,尽可能减少轮询的次数和时间,提高了轮询的效率。

### 1.2 并发扫描

在多端扫描模型中,扫描是一种并发的状态<sup>[5]</sup>。理想情况下,对于每个节点都可以有一个进程/线程同时进行扫描获取数据。但实际上,在工程实践过程中,由于系统资源有限,不能够无限新建进程/线程,更多是根据子网分区域进行多线程扫描,需要复用有限的线程/进程。

多线程扫描流程如图 1 所示,全局节点列表作为跨进程/线程的资源,全局共享。在扫描的最开始阶段,列表只有起始扫描地址。此时,第一个扫描过程 TS<sub>1</sub> 便会扫描该起始节点,并且会将邻接的节点补充到全局节点列表中,从而新建 TS 对邻接节点进行扫描。

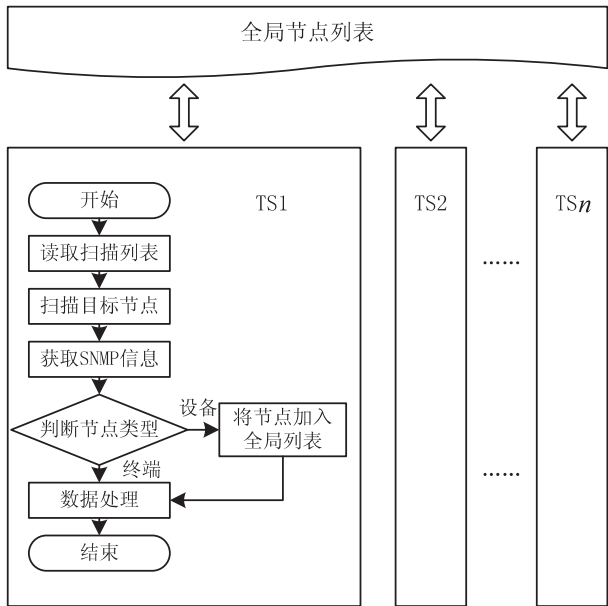


图 1 多线程扫描模型

线程和进程的创建与销毁也是需要系统资源的,

为了复用线程,在 TS 执行完毕后并不会销毁,而是从列表中获取下一个节点进行扫描,在达到系统限定的 TS 数之前,TS 的数目会一直增加。全局节点列表按照先进先出(FIFO)原则组织节点的扫描顺序,节点的扫描先来先服务(FCFS)。

在扫描目标节点阶段,通过 SNMP 获取目标节点的各种信息,比如接口、路由、端口映射以及地址映射等<sup>[6]</sup>。由于这些信息分散在 MIB 中的多个表中,因此可以在扫描阶段细分出多个扫描线程,对这些不同的表同时进行扫描,从而加快扫描进程。在对节点扫描完成后,需要对获取到的数据进行分析 and 整理,完成拓扑结构的确认、检验以及存储,为后续的展现等工作提供数据基础。

### 1.3 拓扑数据获取

扫描的目的和结果都是为了获取拓扑数据,从 MIB 中获取的信息主要有 system 组、接口表、路由表、IP 地址表、网络映射表、MAC-端口映射表、接口-端口映射表这 7 组<sup>[7-9]</sup>,根据这些信息对拓扑进行分析、处理和展现。

## 2 拓扑数据组织与分发

### 2.1 拓扑结构化分析

由大量的终端和网络设备连接起来的网络可以很自然地建模为一张图( $G$ ),每个机器都是一个顶点( $V$ ),而顶点  $u$  和  $v$  之间的直接物理连接则可以看作是边( $E$ )。网络拓扑可抽象为无向图,利用无向图的相关算法对拓扑进行研究,比如拓扑的扫描模型都是基于图的遍历模型而来。图中的边是拓扑中的路由,而图中的顶点是拓扑中的节点,如图 2 所示。

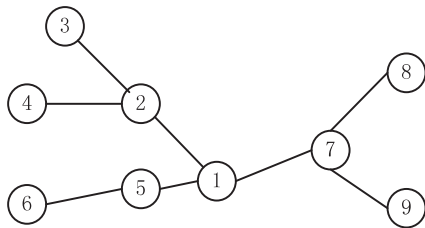


图 2 拓扑的结构化无向图

如果路径中不存在重复的顶点,那么路径便是简单路径,反之则说明路径中存在环路。路径是拓扑中逻辑连接的有限集合,即路由;而环路则说明拓扑的路由存在回路,网络的路由设置存在问题。

如果图中的每一个顶点都存在至少一条边将其与邻接顶点相连,如图 2,那么这样的图便是连接的。当图不连接时,说明相应的拓扑结构出现断裂,出现了逻辑或物理连接上的错误导致了连接孤点的产生。

如果对图中的每条边都附上一个权值,便可知晓一条路径的具体花销,即最短路径问题,并将任意两个

顶点之间的距离都是最短的路径的集合叫做最小生成树。在网络拓扑中,有许多相应的协议以保存拓扑中存在的路由是尽可能最短的,如 RIP、OSPF 以及 BGP 等,自动调整网络路由<sup>[10]</sup>。管理员也可通过静态路由形式手动调整网络的路由。在具体网络中,能够作为权值的指标便是数据传输延时,理想的路由便是最短延时最快传输。

由于获取拓扑数据的过程是逐步扫描的过程,为了表现出扫描的顺序以及拓扑节点之间的逻辑连接关系,可将拓扑的无向图结构转化成一棵有根的树,简称树。在网络中,相邻两个节点之间的关系分为两种:类似于路由器和子网或交换机之间的从属关系以及路由器和路由器之间的邻接关系。判断两个相邻节点之间的关系,是由节点的逻辑位置所决定的。在生成拓扑的过程中,对采集到的节点进行树状形式的安排。需要注意的是,由于拓扑中可能存在路由回路,因此拓扑不是一棵严格意义上的树。

2.2 拓扑存储

为了对拓扑进行存储,需考虑两方面的行为:一是在扫描过程中的临时存储;二是在数据库中的持久化存储。拓扑图中的边的数目远小于顶点数的平方,即 $|E| \ll |V|^2$ ,是比较典型的稀疏图<sup>[11]</sup>,从执行效率和性能来说,更适合使用邻接表。在扫描过程中,可用队列或栈来存储拓扑的邻接表结构。但由于拓扑中节点之间存在逻辑关系,而且这种关系对于拓扑来说非常重要,需要准确记录,因此队列或者栈这种纯集合类型的数据结构对于拓扑来说并不十分合适,需要进行调整和优化。

节点具有天然的对象属性,同时又是扫描时的基本单位,在存储时是以节点为单位,同时节点存在扫描先后的顺序。由于网络拓扑中的路由是双向的,也即是无向的,从节点的角度来看,与它相连的其他节点都可以看作是其下游节点。从而节点结构便可以表示为图3。

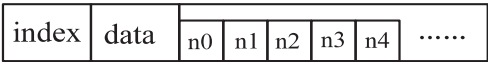


图3 节点数据结构

图中,index 表示节点扫描序号,每个节点都有一个集合存储与其所连的所有其他节点的索引或指针。

假设从节点  $n_0$  开始扫描网络,则整个拓扑在内存中的存储结构便如图4所示。

值得注意的是图4的存储结构可能会存在冗余指针,如图中  $n_3$  和  $n_4$  之间的连接存储了两次,在一定程度上造成存储空间的浪费;但是这种空间的浪费带来的好处是显而易见的,即每个节点都保留有其全部的连接关系,而不用进行额外的遍历查找操作,这种以牺

牲空间换取时间的做法加快和简化了后续的拓扑数据处理。

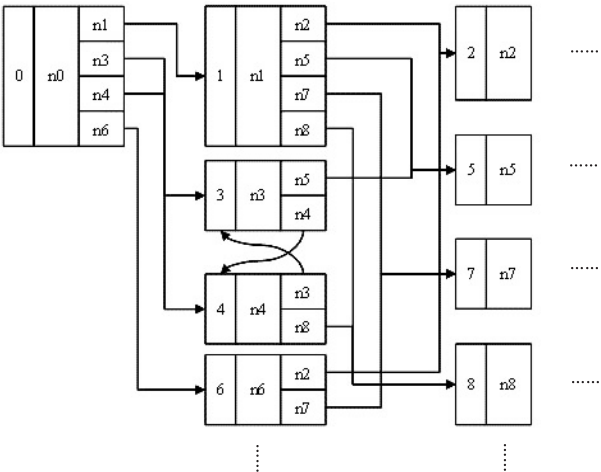


图4 拓扑的内存存储结构

拓扑的持久化存储,是将含有复杂逻辑关系的拓扑转化为以数据库记录为单位的记录集。单独的节点和路由,都可以“个体即为记录”的方式直接存储到数据库中。由于将拓扑的节点和路由作为不同的记录进行切分,导致其天然的逻辑关系被切断,需要额外的工作对此进行维护。另外,存储除了要保证正确,还要考虑到今后提取和使用的方便,所以合理的数据库模型,以及对拓扑进行合理切分并与关系型数据库相映射,是拓扑持久化存储的关键。

2.3 数据发布

在获得拓扑数据并将其存储后,便需要通过一些技术,将数据发布出去。以数据为核心,将数据对外进行发布,以供其他业务组件进行调用的技术可以分为客户端(Client Pull)和服务端推送(Server Push)的两大类。

在网络管理中,拓扑中有许多信息更新的频率很低,比如每个节点的 system 组的信息,在节点初始化安装完毕后就基本上不会对其更新;还有一些情况是虽然数据会经常更新,但是从管理角度来说并不会关注实时变化情况,允许有延时,比如查看全局拓扑。在这些情况下,这些相关信息可以通过“拉”的方式进行数据发布。而像重点局部区域的监控、流量监控、终端违规以及安全风险预警等对实时性要求较高的需求,则需要以“推”的方式来获取相关数据。

在客户端向服务端请求数据的时候,如果当前服务端没有新的数据可以提供给客户端,服务端并不会像传统的“拉”方式一样去发送一个空响应并结束当前请求,而是会将请求保持住,直到有数据更新时便可以立即推送给客户端。而客户端在接收到推送过来的数据后,便又会按正常的流程,再次发起请求,因而服务端时刻都有正在等待的请求可用,并可利用它来及



时地传递数据。

这种有别于传统轮询方式的“长轮询”(Long Polling)就是现在流行的 Comet 技术之一。长轮询本身并不是真正的“推”方式,但是它却能够用来实现实时推送。文中扫描机制便是采用传统轮询和长轮询来实现“推拉”结合的数据发布。

## 2.4 节点状态检测与控制

网络节点的状态是指在网络信息活动中该节点所表现出来的具象和行为,能够被探测、采集和获知的表征数据。当节点接入网络时,无时无刻的数据通信必定会让其留下状态信息,搜集节点的这些活动信息对网络管理来说意义重大。网络中的节点包含终端和网络设备,对于不同类型的节点,所需要检测的状态信息便有所不同。

为了细分并及时获取更详尽的节点连接状态,引入了 SNMP 的 Trap 机制,当特定情况发生时,节点上的 SNMP 代理便会主动给管理端发送 Trap 消息。利用 Trap 机制和扫描分析,从而准确检测终端和设备的状态,达到可控的管理目的。

## 3 网络拓扑结构档案

### 3.1 拓扑档案的构成

所谓拓扑档案便是从时间的维度来看的网络拓扑。拓扑档案的内容是在某个时间条件下的网络状态信息,包括各种终端和网络设备的逻辑连接及其当前运行状态,是拓扑的静态数据特征。

由于网络管理工作需求的多样性,从不同的角度监测拓扑的不同数据特征,就有了不同种类的拓扑档案。结构档案是为了监测拓扑的结构性变化,即拓扑中各节点的逻辑变动;流量档案是为了监测网络中的流量分布和变化;路由档案反映了不同时间的不同的路由策略,路由可以影响到拓扑的整体结构和流量分布,结合前两种档案,便可以分析和优化路由策略。

### 3.2 拓扑档案的更新比对

一个网络在其稳定下来的时候,拓扑结构一般不会出现大的变动,即使有大的变动,那这个变动也是较长久性的,对于后续的变动来说基本是稳定的。在系统初始化的第一次全网遍历扫描时,生成一个基准拓扑。在以后后台进程定时更新拓扑信息时,都会有相应的操作日志,也就是增量更新拓扑而非全量更新。因此,查询任何时刻的拓扑状态,只要取出其增量差值,就能在基准拓扑的基础上展现出该时刻的拓扑。

系统中为了监控网络的状态,会有后台进程定时地对网络进行扫描。每次扫描都会自动更新数据库中的相应信息,并记录下历史记录。反映在拓扑绘制上,便是在树上的局部变动和更新。

### 3.3 拓扑档案的输出

为了方便信息数据的交换和集成,拓扑档案需要有比较好的输出方式,方便用户调阅和使用。由于拓扑数据的复杂,导出成其他格式文档的时候,会丢失一些特性,比如拓扑节点的交互性,因此,在导出的时候需要选择合适的信息,尽可能合理地安排组织好导出的拓扑档案内容。

如果是面向程序的拓扑档案导出,即为与其他程序进行数据交互,选择格式良好的 XML 文档,可以方便地控制导出的内容和格式。同时,由于 XML 文档的可描述性<sup>[12]</sup>,可以非常准确、全面地导出拓扑档案的全部数据,以供其他组件程序使用。

## 4 结束语

网络拓扑状态信息的获取是在网络扫描过程中逐步实现的,文中分析了传统扫描模型的不足之后,提出了多端扫描模型并进行分析。在拓扑状态数据获取之后,根据拓扑的图状特点,对其进行结构化分析,将拓扑的图形结构转变为树形。树形结构的拓扑在扫描过程和扫描完成后,都需要面临存储的问题;在数据存储完成后将数据发布给其他组件进行调用。

### 参考文献:

- [1] 李 津. 大规模网络拓扑生成技术研究[J]. 计算机工程与科学, 2010, 32(3): 11-13.
- [2] Tanenbaum A S. 计算机网络[M]. 第 4 版. 潘爱民, 译. 北京: 清华大学出版社, 2004.
- [3] 李 可, 薛 质, 铁 玲. IP 网络拓扑自动发现研究[J]. 计算机工程, 2004, 30(5): 66-68.
- [4] Stevens W R. TCP/IP 详解 卷 1: 协议[M]. 英文版. 北京: 机械工业出版社, 2004.
- [5] Breshears C. 并发的艺术[M]. 夏雪军, 译. 北京: 机械工业出版社, 2010.
- [6] 叶小涛, 魏海平, 王福威, 等. 基于 SNMP 的网络拓扑发现研究与实现[J]. 石油化工高等学校学报, 2005, 18(3): 82-86.
- [7] 洪正君. 网络拓扑与终端接入状态监测系统研究[D]. 西安: 长安大学, 2011.
- [8] A Simple Network Management Protocol (SNMP) [S]. RFC1157, 1990.
- [9] Wikipedia. Simple Network Management Protocol [EB/OL]. 2011-05-05. [http://en.wikipedia.org/wiki/Simple\\_Network\\_Management\\_Protocol](http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol).
- [10] Forouzan B A, Mosharraf F. 计算机网络教程自顶向下方法[M]. 英文版. 北京: 机械工业出版社, 2012.
- [11] Cormen T H, Leiserson C E, Rivest R L, et al. Introduction to Algorithms[M]. 3rd ed. London: The MIT Press, 2009.
- [12] 蔡昱星. 基于语义 Web 服务的 SOA 系统的设计与实现[D]. 南京: 南京邮电大学, 2011.

# 网络拓扑多端扫描机制的研究

作者：[柴艳娜](#)，[李佳](#)，[CHAI Yan-na](#)，[LI Jia](#)  
作者单位：[柴艳娜, CHAI Yan-na \(长安大学 教育技术与网络中心, 陕西 西安, 710064\)](#)，[李佳, LI Jia \(长安大学 信息工程学院, 陕西 西安, 710064\)](#)  
刊名：[计算机技术与发展](#)

ISTIC

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2013(9)

## 参考文献(12条)

1. [李津](#) 大规模网络拓扑生成技术研究[期刊论文]-[计算机工程与科学](#) 2010(03)
2. [Tanenbaum A S](#). [潘爱民](#) [计算机网络](#) 2004
3. [李可](#). [薛质](#). [铁玲](#) [IP网络拓扑自动发现研究](#)[期刊论文]-[计算机工程](#) 2004(05)
4. [Stevens W R](#) [TCP/IP详解卷1:协议](#) 2004
5. [Breshears C](#). [夏雪军](#) [并发的艺术](#) 2010
6. [叶小涛](#). [魏海平](#). [王福威](#) [基于SNMP的网络拓扑发现研究与实现](#)[期刊论文]-[石油化工高等学校学报](#) 2005(03)
7. [洪正君](#) [网络拓扑与终端接入状态监测系统研究](#) 2011
8. [A Simple Network Management Protocol \(SNMP\)](#) 1990
9. [Wikipedia](#) [Simple Network Management Protocol](#) 2011
10. [Forouzan B A](#). [Mosharraf F](#) [计算机网络教程自顶向下方法](#) 2012
11. [Cormen T H](#). [Leiserson C E](#). [Rivest R L](#) [Introduction to Algorithms](#) 2009
12. [蔡昱星](#) [基于语义 Web 服务的 SOA 系统的设计与实现](#) 2011

本文链接：[http://d.wanfangdata.com.cn/Periodical\\_wjfz201309054.aspx](http://d.wanfangdata.com.cn/Periodical_wjfz201309054.aspx)