文章编号：1005-8451（2018）11-0060-06

# 基于SNMP的铁路信号监督系统网络拓扑发现方法

王　磊，马　亮
（西南交通大学　信息科学与技术学院，成都　611756）

**摘　要：**为了保障铁路信号集中监测系统运行的可靠性，设计一种基于SNMP、ICMP和端口扫描的网络拓扑关系发现方法，自动生成CSM网络设备拓扑图。通过C#语言编程实现并展示了应用该方法生成的网络拓扑图效果。通过本方法，能够快速、准确、全面地发现活动节点物理连接关系，有利于维护人员远程实时监测网络设备运行状态，便于设备故障的定位、分析与维护。

**关键词：**铁路信号监测；SNMP；网络拓扑；STP
**中图分类号：**U284：TP39　**文献标识码：**A

## Method for network topology discovery of railway signal supervision system based on SNMP

WANG Lei, MA Liang
( School of Information Science and Technology, Southwest Jiaotong University, Chengdu　611756, China )

**Abstract:** To ensure the reliability of railway centralized signaling monitoring system (CSM), this paper designed a network topology discovery method based on SNMP, ICMP and port scanning, which could automatically generate the CSM network device topology. This method was implemented through C# language programming to show the network topology generated. Through this method, the physical connection of active node can be found quickly, accurately and comprehensively. It is helpful for the maintenance personnel to monitor the operation state of network equipment remotely, so as to locate, analyze and maintain the equipment fault.

**Keywords:** railway signal monitoring; simple network management protocol(SNMP); network topology; spanning tree protocol(STP)

铁路信号的集中监测（CSM，Centralized Signaling Monitoring）系统是面向高速铁路及普速铁路信号领域的综合性维护支持和信息监控网络平台[1]。根据铁路部门运营管理结构，CSM系统应用“三级四级”的体系结构进行系统部署，铁路局采用交换机组网，车站局域网采用交换机或者集线器组网，电务段子系统则是整个网络信息与服务的汇集地[2]。这些网络设备大多布置在信号机房内，规模庞大复杂，设备之间接口众多，而信号与通信设备若各自独立则不利于进行故障诊断，因此，需要对CSM系统中的网络设备进行集中监测及管理。在信息系统中网络设备之间的通信状态监测依赖于网络拓扑[3]，目的是通过拓扑图直观地反映网络中设备的连接状况，并且可基于网络拓扑实现故障定位、分析和维修[4]，因此，在CSM系统中网络拓扑技术是关键。文献[1]中使用CSM平台对信号设备进行集中监控和智能分析，为铁路信号设备实施“状态修”创造了有利条件，但是，需要对CSM平台本身的网络设备进行监测与维护。文献[5]设计了信息系统综合监控平台，使用ARP表结合ping扫描的方法实现信息系统网络拓扑的自动发现，但是网络拓扑生成时间较长，影响监测的实时性和准确性，而且如果某些设备关闭ping扫描功能，可能会导致扫描不完整，影响拓扑生成的完整性。

本文以保障CSM系统运行可靠性，提高自动拓扑时效性、完整性和准确性为目的，基于SNMP协议，采用网际控制报文协议（ICMP）结合端口扫描的方法全面地探测活动节点，从而能够更有效地发

收稿日期：2018-04-04
作者简介：王　磊，在读硕士研究生；马　亮，讲师。

现 CSM 系统中各网络设备之间的拓扑关系，并可依照生成树原理分析冗余的物理连接，实现自动发现的拓扑与实际网络拓扑一致，最终通过 C# 语言编程实现拓扑自动发现算法。

## 1　网络拓扑介绍

### 1.1　SNMP协议及表单获取

SNMP 称为简单网络管理协议（Simple Network Management Protocol）[6]，是最早的网络管理协议之一。由于 SNMP 被设计成与协议无关，因而得到了众多厂商和网络管理平台的支持，对它进行分析具有重要的意义。SNMP 是一种基于用户数据报协议 (User Datagram Protocol，UDP) 的协议 [7]，可通过 SNMP 协议从路由器中的 MIB Ⅱ信息库或交换机、网桥中的 VLAN-MIB、Bridge-MIB[8] 信息库中获取路由设备列表或主机列表，从而构造网络拓扑。

本文中主要通过 SNMP 获取管理信息库（MIB）变量，目的是通过相关的 MIB 对象判断网络中设备的真实（物理）连接情况，拓扑发现过程中需要获取的 MIB 中的对象详细见表 1 ～表 3。表 1 主要是得到网络中路由器的 MAC 地址以及 IP 地址，表 2 得到交换机转发表中 MAC 地址及对应的端口号，表 3 是获得交换机生成树协议中的端口号、根桥等信息。

表1　ipNetToMediaTable表对象及说明

| 名称 | 说明 | 类型 |
|---|---|---|
| ipNetToMediaIfIndex | 网络设备索引号 | INTEGER |
| ipNetToMediaPhysAddress | 物理地址(MAC) | PhsAddress |
| ipNetToMediaNetAddress | 网络设备IP地址 | IpAddress |
| ipNetToMediaType | 映射类型 | INTEGER |

表2　dot1dTpFdbTable表对象及说明

| 名称 | 说明 | 类型 |
|---|---|---|
| dot1dTpFdbAddress | 物理地址(MAC) | MacAddress |
| dot1dTpFdbPort | 端口号 | INTEGER |
| dot1dTpFdbStatus | 状态 | INTEGER |

表3　dot1dStpPortTable表对象及说明

| 名称 | 说明 | 类型 |
|---|---|---|
| dot1dStpPort | 端口号 | INTEGER |
| dot1dStpPortState | 端口状态 | Integer |
| dot1dStpPortDesignatedRoot | 根桥ID | BridgeId |
| dot1dStpPortDesignatedBridge | 指定桥ID | BridgeId |
| dot1dStpPortDesignatedPort | 指定端口号 | OCTET STRING |

为了方便得到 MIB 变量，在 C# 中可调用针对 SNMP 协议封装的类库 SnmpSharpNet.dll，通过 GetSNMPTable 方法调用封装类库。

关键代码如下：

```
// 配置设备的团体名，IP 地址，版本号等信息。
OctetString community = new OctetString(comm);
IpAddress agent = new IpAddress(ip);
AgentParameters param = new AgentParameters(community);
param.Version = SnmpVersion.Ver1;
UdpTarget target = new UdpTarget((IPAddress) agent, 161, 2000, 1)
// 根据 Oid 找对应的值 Oid rootOid = new Oid(oid);
Oid lastOid = (Oid)rootOid.Clone();
// 采用 GetNext 方式获取，并暂时保存在 temp_list 中
Pdu Table_pdu_next = new Pdu(PduType.GetNext);
List<string> temp_list=new List<string>();
while(lastOid!=null)
{
temp_list.Add(Table_result.Pdu.VbList[0].Value.ToString());
// 找完指定表之后，lastOid 赋值 null
}
```

### 1.2　生成树协议介绍

生成树协议（STP, Spanning Tree Protocol）是一个网桥到网桥的协议 [9]，它随后被 IEEE802 委员会修订并发布在 802.1d 规范 [10] 中。STP 生成树的使用既保障网桥之间的冗余连接，同时又可避免网络环路在交换链路中的出现。STP 基本术语包括：

（1）网桥协议数据单元（BPDU）：STP 中的“hello 数据包”，间隔一定时间（该时间可配置）发送，该消息在各网桥之间交换；

（2）网桥号（Bridge ID）：由 2 字节优先级与 6 字节 MAC 地址组成，为网络中每一台交换机标识身份，优先级为 0–65535，缺省为 32768；

（3）根网桥（RB）：具有最小网桥号，根网桥并

且所有端口都处于转发状态；

（4）指定网桥（DB）：指到根网桥的累计路径花费最小的网桥；

（5）根端口（RP）：网络中在非根网桥上，指定连接到根桥路径最短的端口；

（6）指定端口（DP）：非根网桥为每个需要连接的网段选出一个指定端口，根网桥上的端口都是指定端口；

（7）非指定端口（BP）：非指定端口将处于阻塞状态，不转发任何用户数据。

STP 的主要思想是每个网桥定时发送 BPDU，在冗余网络连接中维持一个无回路的网络，阻塞一个或者多个冗余的接口。当网络中某条链接故障或者添加新的链接，能够快速发现网络链接变化，按照 STP 配置交换机接口，避免丢失链接或新的回路出现。

### 1.2.1　STP工作过程

（1）进行根桥的选取：每台交换机定时向邻接交换机发送 BPDU，选出 Bridge ID 最小的网桥作为网络中的根桥；

（2）确定交换机指定端口及根端口：通过计算非根桥的交换机到根桥的最小路径开销，找出根端口（最小的发送方网桥 ID）和指定端口（最小的端口 ID）；

（3）裁剪冗余端口：阻塞非根网桥上非指定端口以裁剪冗余的环路，构造一个无环路的拓扑结构。

如图 1 所示，根桥 (S1) 选作为树干，在处于稳定状态的网络中，BPDU 从根桥沿着无环的树枝传送到网络的各个网段，没被裁剪的活动链路作为向外辐射的树枝，原本 S2 与 S3 之间有一条链接，图中虚线为阻塞环路，此时 S2 的端口 4 或者 S3 的端口 2 为阻塞状态。经过裁剪冗余之后，生成一颗树结构，树结构是没有环路的。

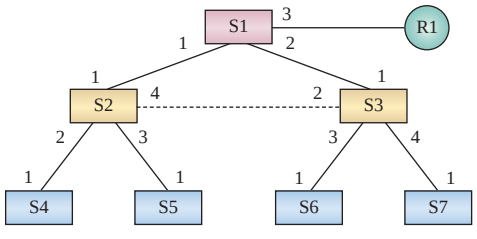


图1　STP协议得到生成树示意图

### 1.2.2　STP操作规则

STP 操作之后，最终确定唯一的生成树，如图 2 所示，A 为根交换机，每个网络中只有一个根桥，根桥上的接口全是指定端口（黄色圈），对于其他非根桥，每个根桥只有一个根端口（黑色圈）；并且每个段只有一个指定端口，其他接口为非指定端口，在图 2 中，C 交换机到 A 交换机，可以通过 C-A 链路，还可以 C-B-A 链路，STP 生成树之后，C 的端口 2 阻塞，那么就只能 C-A，此时该段就只有 A 交换机的 2 端口为指定端口。指定端口才可以转发数据，非指定端口（阻塞端口）不能转发数据。

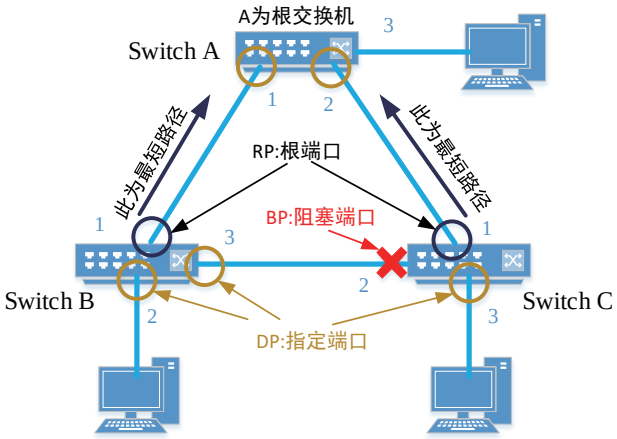


图2　STP工作过程示意图

## 2　网络拓扑方法设计

### 2.1　数据库表单构造

通常在发现网络拓扑过程中会涉及到很多表单，甚至有的表单会多次处理使用，由于各个设备性能也存在差异，如果直接使用 SNMP 协议反复获取路由器、交换机的网络信息表单就会占用更多的网络资源，并且会增加构造拓扑的时间，虽然我们是在局域网中发现网络拓扑，但是需要获取多个设备表单。针对该情况，本文采用本地表单的形式，在数据库中保存当前活动节点以及所有活动节点的网络信息。

（1）需要保存已经探测到的活动节点，表项包括：设备 IP、类型及活动节点标志，用于存放已经被 ICMP 探测或端口扫描出的节点信息；（2）需要一张表存放 ICMP 没有探测到的节点，可用于端口多次扫描使用，表项包括：设备 IP，扫描次数标记。

针对路由器，我们需要获取表 1 中的对象，与

该路由器设备 ID，IP 生成表（设备 ID，路由器 IP，节点 IP，节点 MAC 地址）。

交换机需要获取表 2 及表 3 中的对象，构造转发表（设备 ID，交换机 IP，节点 MAC 地址，节点端口号，节点状态）和 STP 生成树表（设备 ID，设备 IP，Bridge ID，端口号，端口状态，根桥 Bridge ID，指定桥 Bridge ID，指定端口 ID）。

## 2.2 ICMP探测及端口扫描

系统采用 ICMP 结合端口扫描的方式作为拓扑发现的探测机制，避免少数设备屏蔽了 ICMP 功能之后不能被正常发现，导致拓扑不够完整的问题，所以需要通过端口扫描作为辅助方法，结合这两种方式可以更加快速完整地发现搜索范围内的所有活动节点。

设备活动节点的搜索过程如下：

（1）按照管理员要求配置搜索范围，接着由程序通过多个线程同时使用基于 ICMP 的 Ping 方法，针对此范围内的活动节点进行发现，把探索到的节点存入活动节点表中；

（2）针对不响应 ICMP 的节点，进一步使用端口扫描，按照配置文件中的参数可以重复扫描的次数，如果达到扫描次数的上限仍然没有响应就应该放弃此节点，如果在某次扫描中响应，则此节点应该当作被发现的活动节点，加入活动节点表中，待后续数据处理使用。活动节点的扫描流流程如图 3 所示。

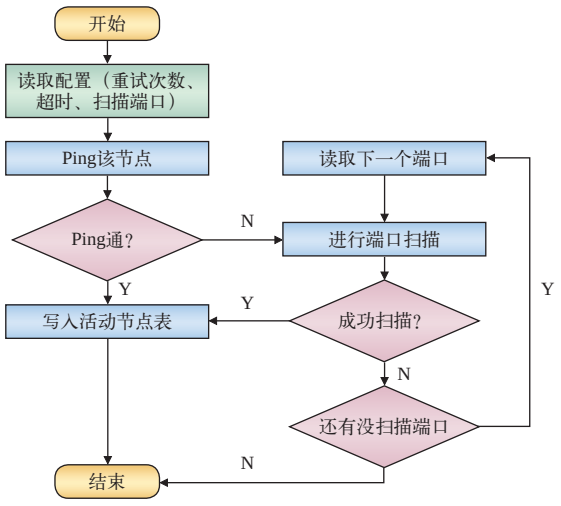


图3　扫描流程图

采用这样的方法可以有效地探测活动节点设备。端口使用了全 TCP 连接的扫描方式，与探测主机搭建一个能够被识别的对应端口的连接，为了节约搜索等待的时间，搜索子模块可同时开启多个线程来进行扫描，并且将搜索发现的活动节点信息全部保存在活动节点表中。

## 2.3 物理连接判断方法

### 2.3.1 物理连接判断

通过 SNMP 协议获取路由器、交换机等网络设备的路由表、转发表数据，虽然转发表记录了节点的 MAC 地址，但是若多台交换机同在一个交换域内，不管节点是否物理连接此交换机，整个交换域内 MAC 地址都会被保存在当前交换机中，所以单纯地根据交换机上的转发表还无法区分此交换机与其他设备是直连的还是非直连的关系 [11]，所以需要进一步通过分析生成树协议，按照生成树的方式来判断设备直连关系。

局域网络中活动节点探测完成后，需要先对各节点进行区分找出各自的类型，并将类型保存在活动节点表单类型中。根据设备类型，可以直接通过 SNMP 协议访问对应需要的 MIB 信息库，也就是得到各路由器 ARP 表及各交换机的转发表和 STP 生成树表。

从上文 1.2.2 中已经知道 STP 操作的规则，可以得出下面几条结论。根据这些 STP 总结的结论，能够确定出根交换机、交换机与交换机、路由器之间的物理端口连接情况。

结论 1：设交换机 S1 的端口标识为 $S1_i$，它的指定网桥为 S2，若在指定网桥上的端口（指定端口）为 $S2_j$，则 S2 必为交换机，且交换机 S1、S2 通过接口 $S1_i$、$S2_j$ 设备直连，并且可以确定 S1 的端口 $S1_i$ 是根端口。

结论 2：若端口上获得节点的 MAC 地址是通过非根交换机的指定端口或者根端口获得，则该 MAC 地址对应的设备属于非直连设备；如果是通过别的端口（处于转发状态）获取，则属于直连设备。因为根交换机所有端口都是指定端口，所以还需要判断是不是与交换机根端口连接，若是，则不是直连，反之则是直连。

结论 3：若阻塞接口的指定网桥是除自身以外的其它交换机，那么该接口必定与其他交换机存在作

为备份使用的冗余链路。

结论 4：设交换机 S 的接口 p 的转发表记为 $A_{Sp}$。对于物理直接连接的交换机 S、K 的两接口 a、b，若 $A_{Sa} \cap A_{Kb} \neq \phi$，则交换机 S 与交换机 K 是通过集线器间接连接，反之，交换机 S、K 是通过接口 a、b 直连。

### 2.3.2　网络拓扑步骤

使用 C# 语言开发程序，在内存中使用存储格式如下。

设备类：

```
String    type    ;        // 设备类型
int       ID      ;        // 编号
char[6]   mac     ;        // 物理地址
long      devIP   ;        // IP 地址
```

端口类：

```
int       ID      ;        // 所属交换机编号
int       PortID  ;        // 当前交换机接口
                              编号
bool      isRootPort ;     // 当前交换机根接
                              口状态标识
int       PortState  ;     // 该交换机接口状态
char      DesignedBridge;  // 该交换机指定网桥
int       DesignedPort;    // 该交换机指定端口
char      linkPart;        // 连接主机或接口
int       LinkType;        // 无连接或直连接
```

网络拓扑步骤如下：

（1）根据交换机 STP 生成树表，找到根交换机，再由结论 1，通过查看表单中的指定网桥，可知道对应的根端口，这样初步找到所有交换机的直连关系，再根据结论 3 找到阻塞端口构成冗余的连接关系；

（2）通过步骤（1）已经找到所有交换机之间的物理连接关系，接下来需要将主机加入到各交换机端口上，根据结论 2，结合交换机转发表中的端口号和 MAC 地址，找到直连的主机，到这里物理拓扑基本上完成；

（3）完成步骤（2）之后，可根据结论 4 找到交换机之间是否存在集线器连接，并在内存的设备信息类中修改设备直连关系。

### 2.4　实现

根据电务段生产力的调整，未来铁路信息化有着更大的需求，依据以数据为中心、通信为依靠的布局，建立网络通信与信号设备为一体的铁路信号综合监测系统。看得出局域网络的正常对各设备之间的通信是至关重要，因此需要对网络中的交换机、路由器等关键设备进行网络拓扑，图 4 是在该系统中应用该方法得到的网络拓扑效果展示图片。用该方法能够快速有效地发现网络中路由设备与各交换机、交换机与各关键设备的物理连接关系，通过拓扑图直观了解网络设备的状况，便于维护人员对设备进行故障分析。

## 3　结束语

本文通过基于 SNMP 的 ICMP 探测并结合端口扫描的方法，实现网络拓扑发现，可减少网络开销，实现网络拓扑发现，完整地发现网络中所有的活动节点，结合 STP 生成树协议能够准确地发现设备之间的物理连接链路，包括冗余链路的发现。但是由于项目需求，本文的方法也存在不足，目前可用于

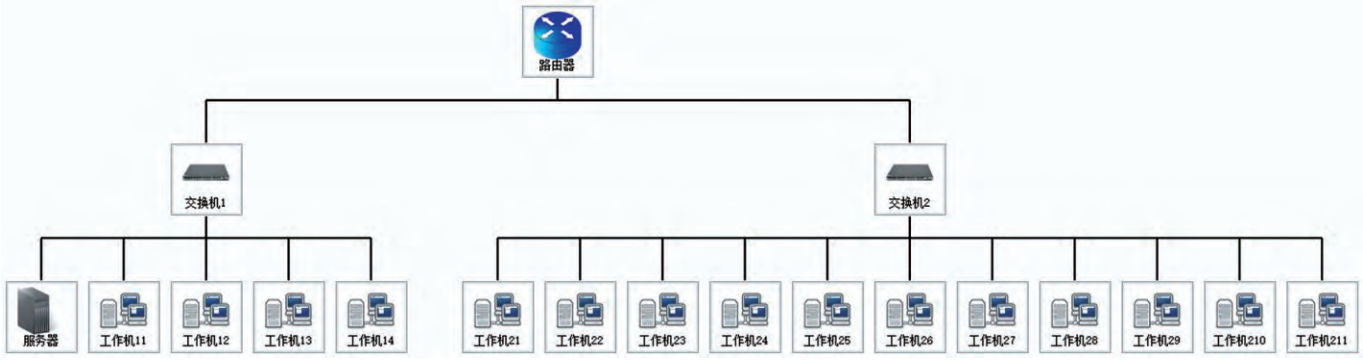


图4　在实际中网络拓扑的效果展示

（下转 P68）

系统每 3 min 要求站内防护员与施工防护员进行“心跳”确认，确认超时将会导致系统记录并报警。

## 5 结束语

本文重点研究了施工作业安全防护方法，从现场需求出发，通过对施工作业安全的流程再造，采用“故障导向安全”的策略，基于 LMD 系统和移动定位技术构建施工安全防护系统，有效降低了施工作业安全风险，最终通过现场应用进行了系统验证，为施工作业人员安全防护提供了有效的解决机制。但可以看到，由于 GPS/BD 在铁路沿线存在盲区，导致无法完全实时获取机车接近位置信息，下一步将重点研究基于智能图像识别技术分析站场机车发车信息，增加安全防护信息来源，以提高系统可靠性。

**参考文献：**

[1] 李东立，许　博，罗建龙，等．普速铁路营业线维修“天窗”管控系统的研究与应用 [J]. 铁路计算机应用，2015（12）：8-12.

[2] 宋修德，邓卫东，李　用，等．基于物联网的铁路施工安全综合防护系统设计及应用 [J]. 铁路计算机应用，2017，26（11）：36-40.

[3] 秦　健．基于北斗的铁路施工作业人员和车辆安全预警防护系统方案研究 [J]. 铁路计算机应用，2017，26（9）：11-14.

[4] 康燕仁．基于红外探测的铁路施工安全防护报警系统 [J]. 电子技术与软件工程，2018（6）：90-90.

[5] 李博绪，田立国，李　智，等．铁路区间施工防护报警系统的设计 [J]. 科技创新与应用，2017（9）：87-87.

[6] 姜　智，胡接旺．列车运行监控设备监测管理系统（LMD）构建与实施 [J]. 铁道通信信号，2017（12）：11-14.

[7] 樊国智．铁路数字化人身安全防护语音提示系统研究 [J]. 铁道运输与经济，2017（b12）：88-93.

[8] 付海娟．基于 GPS 的铁路安全自动防护系统 [J]. 网络安全技术与应用，2015（5）：151-152.

[9] 郭荣昌，林俊亭，李国宁．工务及电务现场作业安全防护系统 [J]. 铁道运营技术，2011，17（1）：4-6.

责任编辑　付　思

（上接 P64）

局域网内的拓扑发现，要想对广域网拓扑发现还需要进一步研究，并结合其他技术手段来实现。针对目前实现的网络拓扑发现，下一步将基于该网络拓扑方法研究网络故障定位，实现综合监测平台的智能故障诊断。

**参考文献：**

[1] 张凤启．信号集中监测智能分析技术的应用 [J]. 铁路计算机应用，2014，23（3）：54-56.

[2] 辛　军．铁路信号集中监测系统研究 [J]. 通讯世界，2016（12）：269-270.

[3] 杨家海．网络管理原理与实现技术 [M]. 北京：清华大学出版社，2000.

[4] 彭　熙，李　艳，王　倩，等．基于网络拓扑结构的智能故障定位系统设计与实现 [J]. 计算机工程，2005，31（2）：219-221.

[5] 刘继全．信息系统运行安全综合管理监控平台的设计与实现 [J]. 铁路计算机应用，2011，20（1）：26-29.

[6] Moon S B, Skelly P, Towsley D. Estimation and removal of clock skew from network delay measurements[C]// INFOCOM '99. Eighteenth Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. IEEE, 2002:227 - 234.

[7] Breitbart Y, Garofalakis M, Martin C, et al. Topology discovery in heterogeneous IP networks[C]// INFOCOM 2000. Nineteenth Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. IEEE, 2002:265-274 vol.1.

[8] 蔡伟鸿，舒兆港，刘　震．基于 SNMP 协议的以太网拓扑自动发现算法研究 [J]. 计算机工程与应用，2005，41（14）：159-163.

[9] 石　玫，李祥和．基于 STP 的物理拓扑发现算法研究 [J]. 计算机工程与应用，2007，43（9）：148-150，204.

[10] IEEE 802.1D-1998 IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Common Specifications Part 3: Media Access Control(MAC) Bridges[S].1998.

[11] 郦金花，李红峰，吉卫红．一种改进的网络拓扑发现方法的设计与实现 [J]. 数据分析与知识发现，2006，1（2）：54-57.

责任编辑　付　思