数字校园网络主干通讯状态自动测试的设计与实现①

康金辉

(陕西理工学院 网络信息中心，汉中 723003)

摘 要：要确认星型结构的以太网所构建的校园网中众多的交换以及它们之间的光连接线路运行是否正常，往往通过查看基于 SNMP 的网管软件或者采用单一的测试方法解决，但这些方法并不能很好满足运行管理的要求。在分析了校园以太网络的连接方式和运行特征的基础上，建立了光连接线路和网络交换形成的单链表数据模型。通过对所有处于管理 VLAN 所在区域的交换机接口 IP 进行自动 Ping 探测以及 TraceRt 探测，并与开源 MRTG 软件获得的流量进行对比分析，实现了对光线路以至两端物理设备运行状态的判断。

关键词：数字校园；以太网；管理 VLAN；光线路；ICMP 协议

Design and Implement of Communication Status Automatic Test of Digital Campus Backbone Network

KANG Jin-Hui

(Network Information Center, Shaanxi University of Technology, Hanzhong 723003, China)

Abstract: To check the connection between a large number of switchings and the optical lines in working order, the network management software based on SNMP protocol is usually checked, or a single test method is used. However, these methods cannot meet the requirements of the operation and management very well. This paper analyzes the features of campus ethernet connection and operation and establishes the singly linked list modal. Finally, it achieves the automatic detection the operation state between the optical line and switch equipment in management vlan regions based on Ping or TraceRt method and makes a comparison with open source MRTG software's flow.

Keywords: digital campus; ethernet network; management vlan; optical line; ICMP protocol

1 引言

校园网承载了多种业务,这些业务依赖于网络基础设施包括交换、路由设备以及光纤线路等。这些设备的运行状态对所承载的业务应用起到重要作用。实际系统中，星型结构的以太网在校园网中得到了普遍的应用。从系统结构上看，多数是具有三层功能的核心交换机连接多个汇聚层，直到接入层。实际应用中，这些设备为数众多，生产厂商往往不一致，要启用基于 SNMP 协议的应用系统来管理整个网络交换、路由设备，实现起来十分繁琐。目前基于 SNMP 网络协议的网管软件通常不能很好地将这些设备统一起来。

汇聚层多个分支连接的基于三层交换设备的网络中，通常划分了许多 VLAN。第三层交换正是基于这些 VLAN 路由通讯而获得了极高的效率。定义了 VLAN 接口静态或者动态接口地址的第三层交换机就会自动把子网内部的数据流限定在子网之内，并通过路由实现子网之间的数据包交换。最简单的情况是管理员配置基于端口的VLAN,并且定义这些VLAN 的IP地址和子网掩码，就产生了路由接口。之后，就可以设置静态路由或者启动动态路由协议实现数据交换。

在核心交换上创建了基于端口的 VLAN 后把网络划分了一个个具有路由接口的子网。这些端口通常通过光纤线路连接第二层交换机，通过在第二层交换机上建立 VLAN 实现 VLAN 透传。如果 VLAN 是建立在具有三层功能的汇聚层上,可以通过启用如静态路由的方法实现通讯。特别指出的是，在以太星型结构

① 基金项目:陕西理工学院科研基金(SLG0922)
收稿时间:2010-04-28;收到修改稿时间:2010-06-10

的校园网环境下，这些连接核心的汇聚层和接入层的交换机数量众多，有的多达上百条链路。而且也要看到，不同的校园网环境其核心结构不尽相同，到汇聚层的连接方式也多种多样，不同厂商的设备互联起来形成一个复杂的网络整体。

要保持这些基础网络环境的正常运行，或者尽可能地减少故障停机的时间，基本的方法是冗余。但冗余的缺点也是显而易见的。但无论是否冗余，都要采用基于 SNMP 协议的网管软件实施监控。当被网管设备采用统一厂商的产品时，其提供的网管软件通常具有较强的功能。但校园网往往经过几期建设，设备种类繁多，甚至有的交换机不支持 SNMP 协议，即使支持，实现起来也十分繁琐，这样就使得统一各个厂商的产品实现全面的校园网管理变得较为复杂。因此，鉴于目前的网络结构和状态，网络管理已经趋向于在网络层实现监控。

应用开源软件 MRTG 可以方便地实现核心到汇聚多个光端口运行及流量的情况[1]，其通用性较好。但 MRTG 的缺点是当网络发生了故障，虽然在流量图上有所反映，但网管人员并不能及时获知。网络运行中存在许多简单的故障情况，如：交换机停电、交换机拥塞、光线路中断（光纤中断、光模块损坏、光跳线中断、光终端机损坏等）、路由错误等等。网管人员希望能迅速发现和定位这些故障；也正如前所述，校园网连接的设备和主干线路众多，发生了一些简单故障，管理员希望不必要手工一个一个简单地应用 Ping、TraceRT 甚至 Telnet 来进行探测，因此，需要一个集中的利用 ICMP 协议的测试系统来自动处理这些问题。系统设计实现的思路是：由于在校园网环境下，二层交换 VLAN 1 是默认的 VLAN，通常作为管理 VLAN（自然也可以用其它 VLAN 作为管理 VLAN，且可以有几个）。配置全网中的所有管理 VLAN 覆盖到全网的每一台交换机，对于 VLAN 同时建立在核心上和汇聚层上实现 VLAN 透传的网络结构来说，通过在管理 VLAN 中的一台网管机，如果在网络中设置不丢弃第二层 Untagged frame,则执行集成设计的 Ping 或 TracerRt 命令，对目标交换机进行逐条光线路、循环、定时探测。对于 VLAN 不是建立在核心而是建立在汇聚层交换上的通过路由技术通讯的网络结构来说，则启用 TraceRt 过程单元。系统根据对目标交换机探测返回的结果，包括返回的字节数、TTL、Round Time 等进行分析以判断当前主干线路通讯是否存在问题。

系统设计中，要设置防火墙策略使其针对具有特定网管 IP 地址的 ICMP 数据包令其“通行”，且其 ACL 不阻止特定管理主机 IP 发送的 ICMP 数据包。这样，ICMP 数据包将被传送到汇聚层以至接入层的任意一个交换机。

鉴于 ICMP 协议的特征，通过调用 Ping 方法或者 TraceRT 方法对目标进行探测时，通常要采用循环、定时的方法多次进行。系统建立了 ACCESS 数据库以存放探测的结果。对于星型结构以太网汇聚层以至接入层以堆叠或者级联方式连接的结构进行分析，系统建立了单向链表结构来存放核心至汇聚层各个连接光纤的编号以及在信息域中存放扫描所需的诸如“连接方式”、“节点型式”等其它信息。

如果在 Ping 或者 TraceRt 方法都不能成功的情况下，系统加大对目标主机探测的次数，若反复探测目标主机没有响应，系统即给出报警信号,并记录于数据库。管理员可以同时查看故障信息表并结合 MRTG 显示的该条线路流量状况，可以对该条网络主干运行的状态作出判断。

2 系统结构及设计方法

小型校园网一般只有单个节点核心，中大型校园网通常具有两个或三个以上节点核心。两个节点的核心间通常采用 MLT 连接或路由连接，三个以上节点的核心连接成环路方式。对于非集中的汇聚节点，一般将 VLAN 建立于核心，通过在核心和汇聚之间 VLAN 方式实现通讯。对于集中的交换节点，通过在汇聚层建立第三层路由交换机应用路由方式实现通讯。对于重要的或者安全性要求较高的一些节点，系统在核心和汇聚节点之间通常架设了防火墙等设备，因此从系统配置上要求从网管工作站能以 Ping 或者 TraceRt 方式发出的 ICMP 数据包到达所有的交换和路由设备并且能够返回。

从光线路连接方式上看，通常有电口级联和光口级联的方式。对于这些情况，同样要求对网管工作站发出的 Ping 数据包做出响应。

为了达到前述的要求，系统根据以太网的特点建立了单向链表结构的数据模型，如图 1 所示。

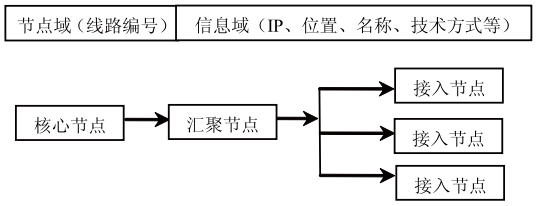

图 1 单链表结构图

如图 1 所示的单向链表结构其信息域存放了代表该节点的“技术方式”、“连接方式”等信息。系统开始运行以前要求通过添加、删除等方法维护这样的链表信息结构，其过程则比较简单。

校园网中从核心到接入层有不同的技术运用和连接方式，这些方式和技术决定着扫描引擎的工作方式。要增加的信息域有：连接光线路的“光束/色谱”，表示处于光缆线路的几号光束，色谱表示使用色谱图中哪两位色谱的光纤，如“红色、棕色”。“连接方式”表示如果从核心到汇聚层交换机直连 Trunk 方式基于 VLAN 通讯，则显示“直连”；如果从核心到汇聚层通过路由技术连接，则显示“非直连”。如果从汇聚层到接入层 Trunk 方式基于 VLAN 通讯，则显示“trunk”。否则，显示“非 trunk”；“节点型式”表示如果从核心到汇聚层连接的汇聚交换机直接连接核心，则显示“远端首节点”；如果以 Trunk 方式连接的接入交换机和汇聚交换机在相同的本地位置，则显示“节点本地”；如果以 Trunk 方式连接的接入交换机和汇聚交换机不在相同的本地位置，则显示“远端次节点”。技术方式表示从核心到汇聚采用 VLAN 技术还是路由技术。如表 1 所示。

表 1 节点域的详细表示

序号	楼宇名称	光路编号	IP	光束/色谱	连接方式	节点型式	型号	技术方式
1	1 号楼	1	192.168.66.6	1/1-2	直连	远端首节点	神码	VLAN
2	2 号楼	2	192.168.66.7	1/1-2	直连	远端首节点	中兴	VLAN
3	3 号楼	3	192.168.66.8	1/1-2	直连	远端首节点	北电	VLAN
4	3 号楼	3	192.168.66.9	1/1-2	Trunk	节点本地	北电	VLAN
5	3 号楼	3	192.168.66.10	1/1-2	Trunk	节点本地	北电	VLAN
6	4 号楼	4	192.168.66.11	1/1-2	非直连	远端首节点	思科	路由
7	4 号楼	4	192.168.66.12	1/1-2	Trunk	远端次节点	思科	VLAN

系统工作时，顺序扫描链表中的每个节点，从链表中的信息域取出代表该节点的所有信息存放到数组，从光路编号取得光路的顺序号，顺序循环扫描单向链表节点，根据信息域中的标识控制扫描过程中的动作。如表 1 中的第 3 条光路，扫描节点域得到该光路连接三台交换机。第一条“直连”核心，“VLAN”方式，启动扫描引擎到第一个 IP “192.168.66.8”；之后，从“光缆编号”、“连接方式”和“节点型式”发现该节点仍然存在于第 3 条光路，且是“节点本地”，这时继续从第 3 条光路启动扫描到 IP“192.168.66.9”；之后，同样的过程再次扫描第 3 条光路，扫描到 IP“192.168.66.10”,完成整个该光线路所连接网络的扫描。特别要指出的是，在扫描过程中要根据标识“VLAN”，“路由”来决定启动 Ping 模块或 TraceRt 模块，并且根据返回的数据包解析结果来决定是否采用重复扫描和增加数据包的大小或者 TTL 时间。

正常情况下，扫描得到返回的结果，包括返回时间、包大小、TTL 等。但当系统发生了“超时”，系统将加大探测的次数。例如：系统发包 10 次，第一个包超时，但随后发送的 9 个数据包，都有正常的返回结果，因此，可以判定系统工作正常。只有当发送了 10 个包，都发生“超时”，则判断系统可能发生了故障，将当前所扫描的信息存放到 Access 数据库中，同时给出报警信号。管理员可以从最近的一次整体扫描过程中可得知发生故障的时间、地点、远端首节点、节点本地、路由、VLAN 等信息。从而能及时处理故障，减少网络故障的时间。

从数据库结构设计看，系统设计有两个表，一个是网络信息表，其结构大致和表 1 的结构相同，不过其中增加了“交换机物理位置”、“单模多模”、“用户 IP 范围”、“计费策略”等字段，以便管理员在查看在该网络发生

故障时，将这些信息传送到“故障信息表”，借以判断网络中的某些物理或逻辑故障。另一个表是“故障信息表”，故障信息表由扫描过程产生，除了记录发生故障时发生的时间、地点、光路编号、楼宇名称、IP、连接方式、节点型式等信息外，还记录了网络信息表中“物理位置”、“单模多模”、“计费策略”等信息。这些信息正常情况下录入，故障发生时一并显示出来。

3 扫描模块设计

扫描过程的设计包含两个设计模块，一是 Ping 函数，二是 TraceRt.设计的方式是利用 Windows 提供的 ICMP.DLL 调用 API 函数设计实现[2,3]。在以 Delphi 表示时，其函数是：

```
Return_packets:=IcmpSendEcho(
hICMP,FIPAddress,pReqData,Length(MyString),nil,
pIPE,BufferSize,FTimeOut);
```

其中:

hICMP: Thandle， //ICMP 句柄；

FIPAddress： inet_addr(PChar(HostIP)); //转换为 inet_addr 地址形式；

pReqData：//指向发送 ICMP 数据包数据载荷的指针,其值为 pchar(MyString) ；

Length(MyString)：发送数据包的长度；

pIPE：PIcmpEchoReply;//ICMP 回应数据包缓冲区指针；其结构是：

```
其中 TIcmpEchoReply = packed record
        Address: DWORD;
        Status:  DWORD;
        RTT:     DWORD;
        DataSize: Word;
        Reserved: Word;
        Data: Pointer;
        Options: TIPOptionInformation;
        end;
```

使得：PIcmpEchoReply = ^TIcmpEchoReply;

BufferSize：回应数据缓冲区的大小；

FtimeOut：超时时间。

当 Return_packets=0 时，表示在规定的 FtimeOut 时间内没有数据包回应。否则，从回应的数据包指针 pIPE 解析获得对方主机的 IP 地址 Get_HostIP。若 Get_HostIP 等于发送时的 IP 地址，则通过 pIPE 指针详细解析即可获得所需结果如下：

```
Get_HostIP:=StrPas(inet_ntoa(TInAddr(pIPE^.Addr
ess)));
```

收到的字节数：IntToStr(pIPE^.DataSize)

TTL: IntToStr(pipe^.Options.TTL)

Round Time: pIPE^.RTT

实现 TraceRt 的核心方法仍然是利用 ICMP 协议。首先设远端目的主机 IP 为 IP1,最大 30hops，第一次发送时设 TTL 为 1,从返回数据包解析得 IP2,如果不等于“0.0.0.0”且不等于 IP1,则以 IP2 为目的地址发送数据包三次，TTL 为最大；解析返回的数据包，如果等于“0.0.0.0”，则超时，如果不等于“0.0.0.0”，则根据返回的数据包解析其所含数据内容。第二次设发送的 TTL 为 2,继续解析得 IP2,若为“0.0.0.0”，则超时，否则，且不等于 IP1,则以此时的 IP2 为目标地址发送三次，以此类推，直到最大 30hops 或者解析得 IP2=IP1 结束。

系统设计中，由 Ping 以及 TraceRt 对目标主机的测试并不是充分条件，实际运用时，要结合 MRTG 对某条线路实时流量进行分析[4]，当系统能通过扫描模块得到某条线路工作正常时，表明该条线路物理上或者逻辑上能够通讯，但其业务 VLAN 并不一定通讯正常，因此要结合 MRTG 进行分析；但当扫描得到线路不正常时,如果从 MRTG 见到该 VLAN 区域流量正常，表明管理 VLAN 数据可能不正常，只有在扫描得到异常，且从 MRTG 上看到系统流量异常之时，可以判定系统已经发生故障。然而，校园网的运行经验表明，在大多数情况下，主动扫描得到的数据可以作为该区域网络工作正常与否的判据。对于物理层发生的故障可准确判定，对于第二层至第三层故障仍然要结合 MRTG 或者其它网管软件加以判定。

4 结语

利用文章提出的方法应用 Delphi7.0 设计工具结合 ACCESS 数据库进行开发，在我校北校区校园网进行了充分的测试。管理机设于 VLAN 1 环境，第三层交换 VLAN 可路由。设定防火墙、全网路由交换机、服务器等设备针对特定管理机 IP 地址的 ICMP 消息协议不禁止。网络共计 43 条直连光路，58 个 Trunk 链路，3 个路由节点，3 条室内多模短

（下转第 226 页）

启发式规则的扩展和改进，其特点和优势主要体现在两个方面：

(1) 服务器端应用程序的改进。重写 URL 涉及到服务器端应用程序的修改，在服务器端 Web 应用支持 Cookie 的情况下，采用重写 URL 的用户跟踪方法，即使用户浏览器禁止 Cookie 的使用，服务器端仍然能够准确的识别每个用户。这是 IASR 用户识别算法的前提，只有每条日志记录都包含会话 ID，才能准确的实现 IASR 用户识别操作。

(2) 引入会话（Session）识别用户。通过服务器端应用程序的改进，日志记录中均包含有会话信息。IASR 用户识别算法将三条启发式规则扩展成为四条判断规则。当两个用户具有相同的 IP 地址和用户代理时，不是直接采用路径分析方法，而是先进行会话判断，如果这两个用户的会话 ID 相同，直接断定他们为同一用户；否则，再进行路径分析。

目前大多数用户识别算法都需要 Cookie 的支持，然而，IASR 用户识别算法摆脱了对 Cookie 的依赖，提高了用户识别算法的通用性。它还引入会话识别，能够高效准确地识别通过同一代理服务器访问站点的用户和直接在浏览器地址栏输入 URL 信息访问站点的用户。尽管如此，用户识别还存在一些亟待解决的问题。比如，同一用户使用多种浏览器访问站点的情况，本地缓存造成的日志记录不完整等问题。就当前存在的这些问题，可以看出用户识别算法还具有较大的发展空间，其发展趋势包括两个方面：(1)提高用户识别算法的有效性和准确性。基于经典的三条启发式规则，增加新的识别条件或者改进服务器端应用程序，提高用户识别算法的效率，增加用户识别算法的准确性；(2)突破三条启发式规则，提出创新算法。目前的用户识别算法都被三条启发式规则所束缚，要推动 Web 日志挖掘领域的发展，必须突破现有的算法模式，从新的角度提出用户识别算法。

参考文献

1 赵伟,何丕廉,陈霞,谢振亮.Web 日志挖掘中的数据预处理技术研究.计算机应用,2003,23(5):62－65.

2 熊忠阳,周亚峰.Web 访问挖掘的预处理技术的研究.计算机技术与发展,2007,17(8):11－15.

3 Pirolli P, Pitkow J, Rao R. Silk from a Sow's Ear: Extracting Usable Structures from the Web. CHI-96, Human Factors in Computing Systems, 1996.

4 李煊,庄镇泉.Web 访问挖掘预处理的用户识别算法.计算机工程与应用,2002,38(7):173－176.

5 陆丽娜,杨怡玲,管旭东,魏恒义.Web 日志挖掘中的数据预处理的研究.计算机工程,2000,26(4):66－68.

6 吴强,梁继民,杨万海.Web 日志挖掘预处理中的用户识别技术.计算机科学,2002,29(4):64－66.

7 方成效,袁可风.Web 日志挖掘的数据预处理研究.计算机与现代化,2006,(4):79－82.

8 孙卫琴.Tomcat 与 Java Web 开发技术详解.北京:电子工业出版社,2009.

（上接第 116 页）

线路连接，15 台服务器，逐条光线路、定时光线路、循环光线路自动测试和人工测试，数据都能得到及时响应。设定故障点人工测试和本软件自动测试都能及时报警并显示。系统运行了大约 3 月后，发现有一台远端交换机经反复测试无法通讯，经现场查看发现，交换机柜风扇停机，交换机无法充分散热造成交换机故障，从而将故障及时排除。但不可否认的是，由于要利用 ICMP 协议，因此要使得系统正常工作，必须使到目标主机的设备不能阻止 ICMP 数据包，一定程度上造成网络潜在的不安全性。此外，系统也没有充分利用目前基于 SNMP 协议的图形化软件界面的优点，各条线路的流量并不是按照 SNMP 协议获得[5,6]等都使得系统显得不直观，有待于进一步研究。

参考文献

1 陈东,邓鸿.MRTG 在监控网络主干状况的应用.潍坊学院学报, 2005,5(4):35-36.

2 杨龙江,高静.图形化方针 PING 命令的设计.电脑编程技巧与应用,2003,9:22-24.

3 马金虎.VisualC#创建 TraceRt 命令.电脑编程技巧与应用, 2004,10:49-51.

4 刘小明.MRTG 日志文件的分析研究.电脑学习, 2007,6: 22-23.

5 贾志强.基于 TCP/IP 的流量检测技术.中国石油大学胜利学院学报, 2007,21(1):14-15.

6 卢苇,严斌宇,郑畅.MRTG 在校园网状态检测参数中的应用.四川大学学报(自然科学版), 2007,38(2):189-191.