文章编号：1005－8893（2002）02－0043－04

校园网络拓扑监控研究*

封红旗[1]，符彦惟[1]，王娟琳[1]，徐晓华
（1. 江苏石油化工学院 现代教育技术中心，江苏 常州 213016）

摘要：随着校园网规模的日益扩大，网络管理是十分重要的，网络拓扑发现与监控是网络故障管理和安全管理的基础。通过 TCP/IP 的 ICMP 报文协议进行 IP 节点的拓扑监控，通过与绑定的地址对进行 IP 合法性检测，并对校园网的服务器进行故障监测。

关键词：网络管理；拓扑结构；IP 地址；ICMP；DELPHI；API
中图分类号：TP 313.18　　文献标识码：A

随着 1995 年 12 月 CERNET 一期工程的验收，全国高校都建立起了自己校园网络。经过几年的努力 CERNET 规模不断扩大，我校的网络规模也随之扩大，应用的增加，给网络管理者提出了新的课题，如何才能管理好，维护好我们精心构建的网络？如何才能充分利用它，发挥最大的效益？网络的应用越来越广泛，随之而来的网络管理也越来越复杂，越来越困难，仅仅依靠手工及系统提供的有限的工具来实现网络的管理是不够的。因此，开发网络管理工具十分必要。

1　系统设计分析

1.1　网络拓扑监控作用

网络监控是网络管理几大功能的基础[1]。网络的安全管理功能需要对网络上所联结资源进行特别配置并对一切网络活动进行监控，才能建立网络上的安全机制。监控网络设备和连接的当前使用情况对性能管理是至关重要的。得到的数据不仅能帮助管理者立即分离出计算机网络中正在大量使用的部分，更重要的是，利用它可以找到某些潜在的问题。网络监控还对网络故障管理进行诊断与发现，在网络中某处发生故障时，网络监控可以及时把信息通知给管理员。图形化的网络拓扑结构使网络管理员可以迅速方便地发现局域网上出现故障的节点资源并帮助管理员分析故障原因。当网络中的 IP 节点不合法，机器死机或各链路断掉，便于网络管理人员发现诊断。网络拓扑图是网络监控的有效帮助，拓扑图的发现更便利了网络的监控。

1.2　课题分析

我校的校园网 1997 年已进入 CERNET 华东北地区，分配到 24 个 C 类地址。校园网中利用路由器和三层交换机来划分网段，网段中的每个用户通过相应的主机地址来进行划分。由于路由器的端口数在绝大多数情况下无法做到每个端口一个节点，于是不可避免地存在 IP 地址盗用的问题。从而为园区内的网络管理和计费等问题带来很大的影响。因此本课题主要解决校园网中主机节点的监控与合法性检查。同时根据检测到的节点状态，我们给出拓扑图，同时也方便了对主机节点的监控。

1.2.1　拓扑图实现

由于主要是对节点的状态检测与监控，因此对于拓扑图的实现只要在给定的子网中确定已发现的 IP 节点的状态，根据当前节点的状态画出拓扑图。对于一个子网的拓扑，主要利用的是 TCP/IP 中 ICMP 协议，发现其节点的状态，给出拓扑图。另

* 收稿日期：2001－11－22
作者简介：封红旗（1967－），男，江苏泰兴人，讲师，主要从事计算机网络管理与维护方面的研究。

外可以按照局域网中工作组分类给出网络拓扑结构，拓扑显示所有的工作组和工作组下的主机情况。

1.2.2 IP 地址的检测

在网络中，每台主机或者是路由器都有一个全网唯一的地址。该地址就是一个用 4 字节表示的逻辑地址，与硬件没有关系。网络层利用 IP 地址相互识别与通信。管理员的计算机可以向目标 IP 计算机发送一个 ICMP 回应请求包，目标计算机如果收到了，则会将网络包回传给管理员的计算机。这样，用户计算机就可以知道目标主机是否存在。

1.2.3 IP 地址管理

由于网络是有偿使用的，所以就存在了盗用 IP 的可能。因此有必要让用户严格地使用网络中心分配的 IP 地址，要做到这点，采用的是把用户的 IP 和用户网卡的 MAC 地址在路由器中绑定的办法。在一个以太网内数据的传输依靠是 MAC 地址。在网段的路由器上有 IP 和 MAC 的动态对应表，这个表由 ARP 协议动态生成并维护的。配置路由器时，可以指定静态的 ARP 表，这样，路由器会直接用静态 ARP 表中的 MAC 地址封装数据，如果目的计算机的 MAC 地址与路由器 ARP 表中的 MAC 地址不一致，那么目的计算机就无法正确接收数据。而计算机的 MAC 地址是由网卡决定的，每块网卡的 MAC 地址都是唯一的，这样可以防止本网段的 IP 地址被盗用。绑定 MAC 地址的操作是在路由器上完成的。

1.2.4 服务器状态监测

校园网中的各个服务器提供了许多服务。HTTP 服务器提供了 WEB 资源，每个服务器站点都运行服务器程序监听 TCP 的 80 端口，等待客户端发过来的连接。在建立好连接后，每当客户发出一个请求，服务器就发回一个应答，然后释放连接，在浏览器和 WEB 服务器之间的请求与应答用的协议叫 HTTP 协议。

FTP 服务器，提供了服务器上资源的下载，用户还可以把本机资源上传（这要求有一定的权限）。FTP 具有严格的权限控制，在请求传输文件之前，要求客户必须向服务器注册用户名和口令。服务器对用户名和口令进行验证，拒绝非法用户的访问。但对于免费的共享文件，FTP 提供了匿名 FTP 的访问方法。建立控制连接时，由客户向服务器发出建立连接请求，服务器使用 21 端口号建立 TCP 连接。

SMTP 服务器，提供了邮件的发送。电子邮件是因特网上使用的最广泛的服务。SMTP 是两个消息传送代理 MTA 之间的通信协议。发信方发送邮件时由用户代理软件将邮件送到消息队列。使用 25 端口号在源机器和目的机器间的 SMTP 服务器之间建立 TCP 连接。

1.2.5 其 他

作为一个网络管理类的软件，应该能获取关于远程主机的更多信息。比如获取它所在的工作组，还可以获取它是否有共享信息，到达这台远程主机所经过的路由，这样当发现问题可以有更详细的主机信息。

1.3 设计目标

通过以上分析，本课题需要实现如下目标：①网络节点的自动检测：检查校园网中存在哪些已存在的节点，并建立一个存在的节点 IP 表，这是网络监控的基础。②网络节点的状态：监测某一节点当前的状态，即是否是活动的。也可以监测整个网段当前所有已存在节点的状态。③网络拓扑显示：根据监测的整个网段节点状态，画出拓扑图。④IP 地址追踪：检测此 IP 节点的信息，最主要的是 IP 地址的合法性。⑤IP 和 MAC 地址对的绑定：建立和维护绑定地址对 IP－MAC 表。用于 IP 合法性检查的对照。⑥服务器状态监测：对网络状态的监测，不仅需对节点的监测，还需要对服务器的状态进行监测，以便提供更好的服务。⑦故障通知：发现故障能及时的给管理员发送通知。

系统设计总体结构图见图 1。

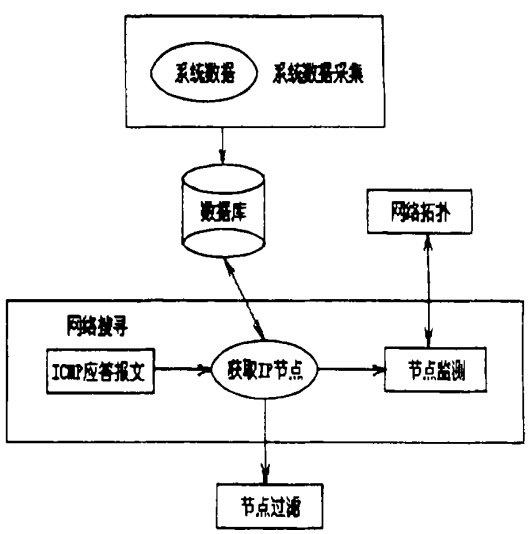

图 1 系统设计实现图

系统实现示意图见图 2。

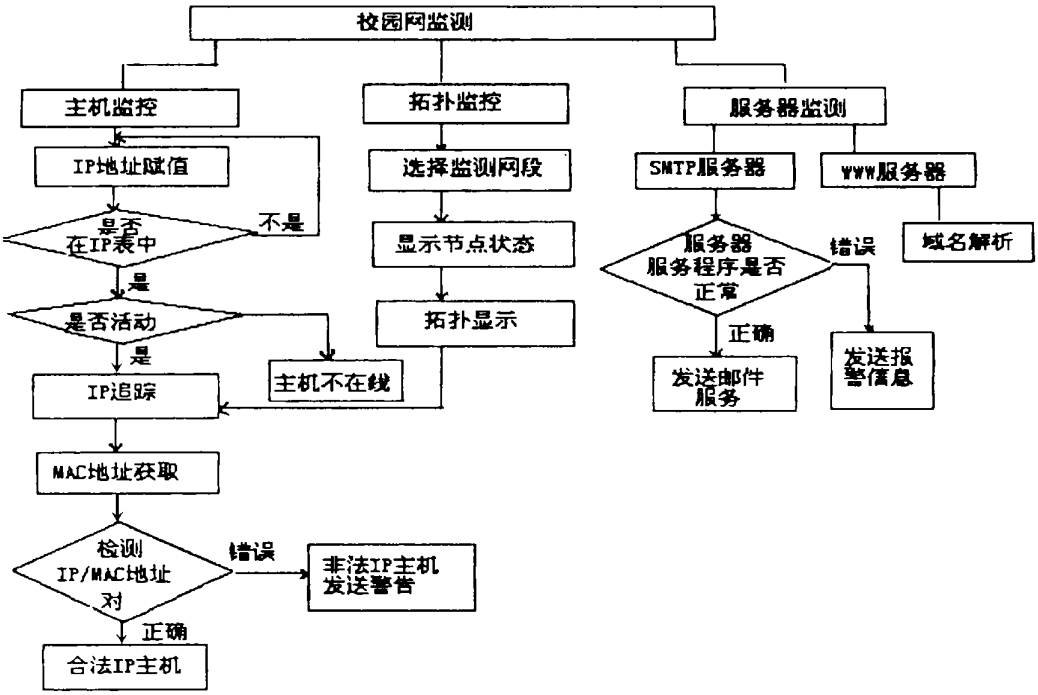

图 2 系统实现示意图

2 校园网主机节点检测

本模块是通过 ICMP. dll 中的函数调用实现的。ICMP 协议是本系统实现的关键[2]。下面介绍在本程序中用到的一些重要和基本的函数。关于 ICMP. dll 中的 3 个 API 函数:

(1) IcmpCreateFile MSDN 定义 HANDLE WINAPI IcmpCreateFile (VOID), 作用是创建句柄, 通过此句柄 ICMP 请求能被处理。成功则返回已句柄。失败则返回 INVALID_HANDLE_VALUE。

(2) IcmpCloseHandle MSDN 定义 BOOL WINAPI IcmpCloseHandle (HANDLE IcmpHandle), 作用是关闭由 IcmpCreateFile 创建的 ICMP 句柄。成功则返回真, 否则返回假。

(3) IcmpSendEcho MSDN 定义 DWORD WINAPI IcmpSendEcho (

HANDLE IcmpHandle // IcmpCreateFile 创建的 ICMP 句柄

IPAddr DestinationAddress //响应的目标 IP 地址

Lpvoid RequestData //包含所要发送数据的缓冲区

Word RequestSize //RequestData 缓冲区中的字节数

PIP_OPTION_INFORMATION RequestOption // 指向请求的 IP 头信息的指针可以为空

Lpvoid ReplyBuffer //存储远程机对本地 ICMP 请求响应所返回的数据, 函数正确返回时, 此缓冲区包含一个或若干个 Icmp_ECHO_REPLY 结构, 后面是一些选项和数据

Dword ReplySize // ReplyBuffer 缓冲区的大小。此值最小要能包含一个 ICMP_ECHO_REPLY 结构大小外加 8 个附加的字节 (即 ICMP 错误信息的大小)

Dword Timeout //等待响应时间

本模块是系统的核心部分, 也是系统的主界面, 在这个主界面就它实现了 4 个强大的功能, 即自动检测节点, 监测指定节点状态, 查找某个网段中节点状况, 拓扑显示网络状况。

2.1 自动检测节点

选择网段和要查找的节点范围后, 可以自动检测这些节点是否活动, 并且显示检测到哪些 IP, 加入 IP 数据表中, 并用于以后的监测与拓扑显示的源数据。

2.2 监测指定节点

输入需要查找的 IP 后, 如果该 IP 节点已经是存在的 (即在 IP 表中), 并且当前也是活动的, 则在表中以绿颜色显示; 如果当前不在线的则在表中以红色显示。如果该 IP 原来没有发现的, 当前是

活动的，则加入 IP 表中（成为一个存在的 IP），并且绿色显示；否则就是不存在该 IP 节点。查到此 IP 是活动的可以进一步追踪。

2.3 拓扑图

确定需要查找的校园网的某个网段，就会显示这个网段中已存在的节点的状态，如果当前是活动的绿色显示，如果不是线则红色显示。并且可以拓扑显示所查找网段的节点状态，点击拓扑显示后，可以简洁明了的看到整个子网的总线型拓扑图，整个网段的节点状态轻松获得。同时也可以开启自动刷新，系统自动刷新显示当前节点状态。

3 校园网监测

这是本系统的另一个主要部分，包括对第一部分的 IP 监测的结果进行进一步的追踪与检测。还包括对各种服务器状况的测试与使用。测试校园网内几个服务器当前状况，是否服务器发生故障，这样可以及时进行修复。

3.1 IP 追踪

对校园网 IP 监测的结果进行进一步的追踪，分别获取它的 MAC 地址，计算机名，所属的工作组，到达此 IP 所经的路由，是否有共享信息。获取 MAC 地址后，可以与绑定的 IP 和 MAC 对比较，判断此 IP 是否合法。

3.2 IP 和 MAC 绑定

建立和维护 IP－MAC 数据库表。点击导入可以把从路由器中下载的文本文件经过过滤导入到表中。此外对每个按钮都提供了确认框，防止误操作，引起不必要的麻烦。

3.3 服务器

检测 HTTP 服务器是否发生故障，并且还有域名解析功能。浏览主页则调用当前默认的浏览器进行 web 浏览，方便了本系统的使用者。对 SMTP 服务器检测是否发生故障。当服务器程序正常工作，我们还可以用来进行发送邮件。当校园网中其他服务器发生故障或监控的 IP 节点主机不合法时，我们可以用此来发送特定邮件给其他管理员，及时进行处理。

4 结束语

网络管理是计算机网络的一个十分重要的问题，也是一项综合性，比较复发的工作，为了实现一个有效的网络管理，除了需要网络管理人员对网络管理系统的结构、原理、网络管理平台有比较清楚的了解外，还需要熟悉网络中的各种设备，而且对各种网络管理协议都要有比较深刻的理解。要建立一个能够真正发挥作用的网络管理系统，需要网络管理者付出很多劳动。

参考文献：

[1] [美] 马塞厄斯·海因，戴维·格里菲思. 简单网络管理协议的理论与实践 [M]. 北京：国防工业出版社，1999.4

[2] 徐新华. Delphi5 高级编程 [M]. 北京：人民邮电出版社，2000.176

The Research on Campus Topology Monitor

FENG Hong－qi[1]，FU Yan－wei[1]，WANG Juan－lin[1]，XU Xiao－hua

（1. The Center of Mordern Education Technology，Jiangsu Institute of Petrochemical Technology，Changzhou 213016，China）

Abstract：With the development of campus network，it is important for us to manage the campus network. The network topology discovery and spy is the foundation of network malfunction management and security management. Through TCP/IP and ICMP Protocol we can discover and monitor the IP node. Compared with the binding IP and MAC address，we can check if the IP address is valid，check the IP node′s state and draw Topology structure. In addition we monitor the campus network servers. The manager can use the Topology structure to find the campus network node′s state and the sub campus network′s state. If campus network is down，this system can send messages to manager，then the manager can find the problem and solution.

Key words：network management；topology structure；IP Address；ICMP；DELPHI；API