

局域网计算机状态自动检测的设计与实现

高成敏 陈良 (广州广东警官学院 计算机系 510232)

摘要:本文设计了一种自动检测计算机状态(包括计算机是否启动,网络是否联通)的方法,并给出可能有故障的计算机列表。采用 ICMP^[1](Internet Control Message Protocol, 互联网控制报文协议)检测计算机状态,并用 Access 数据库进行记录,用 C++ 语言在 VC++6.0 环境下实现了这种方法。局域网(机房)维护人员可随时检查可能有故障的计算机的列表。该方法及其实现软件对减轻局域网(机房)维护人员的工作具有很大的实用价值。

关键词:ICMP 协议 计算机状态 自动检测 局域网

1 前言

本人作为一名高校计算机局域网(机房)的管理维护人员,负责维护 7 个机房,每个机房 39 台电脑,由于有些电脑设备老化,使用频率又非常高,电脑故障经常发生,而检测有故障的电脑要逐一打开每台电脑,工作量非常大。能否设计一种方法自动检测并列出可能有故障的电脑?只对可能有故障的(疑是故障)电脑进行确诊,这样避免了对全体电脑的检查,大大减少了故障检查的工作,又不影响教学的正常进行。

2 高校机房局域网管理维护分析

机房局域网管理现状:教学用计算机使用频率高,有些计算机设备老化经常出现故障。

机房局域网使用需求:保证教学用计算机正常工作。

现实与需求的矛盾:故障及时检测与排除的巨大工作量和有限的人力资源的矛盾。

解决方法 1:局域网管理维护人员打开每台电脑检查计算机的状态。缺点:工作量大,消耗能源,确定故障计算机很耗时,很难保证教学用计算机故障及时检测与排除。

解决方法 2:教师在上课时发现有故障计算机及时登记,局域网管理维护人员按登记维修。缺点:有些教师不习惯或没有时间登记,等到计算机不够学生用才想登记为时已晚。

由于以上两种方法的缺陷,能否设计一种新的方法,不用教师登记也不用局域网管理人员打开每台电脑进行检查,便能知道哪些电脑可能有故障,只检查这

些非常少的可能有故障的电脑。这样矛盾解决了,同时克服了以上两种方法的缺点。

3 局域网计算机状态自动检测方法的设计

在教师上课的时候,每名学生会启动一台电脑,设这些电脑的集合为正常电脑集合 S_c 。设机房内的全部电脑集合 A_c ,那么没有启动的电脑集合 $P_c = A_c - S_c$ 。这个集合中的电脑就是有可能有故障的电脑。设集合 S_c 的元素个数 $|S_c|$,全部电脑集合 A_c 的元素个数 $|A_c|$,则可能有故障的电脑集合的元素个数 $|P_c| = |A_c| - |S_c|$ 。这样只检测 $|P_c|$ 台电脑而不是 $|A_c|$ 台电脑,就可检测出该机房有故障的电脑。将集合 S_c 记录下来,并求得 $P_c = A_c - S_c$ 即可。

改进一:如果一天中的每一次课(1,2 节、3,4 节、5,6 节、7,8 节,晚上)都进行记录,正常的电脑集合 $S_{12}, S_{34}, S_{56}, S_{78}, S_{晚}$,则它们的并集 $S_c = S_{12}S_{34}S_{56}S_{78}S_{晚}$, $|S_c|$ 将更接近 $|A_c|$, $|P_c| = |A_c| - |S_c|$ 将进一步减小(最小为即所有计算机都正常,不需要检查)。如果一天之内一次也没有启动过的电脑有故障的概率则非常大,但数量却很少。逐一开机检查集合 P_c 内的计算机的操作系统和网络联通状态,与开机全部计算机检查相比,耗时将大大节约。

下面给出一个简化的局域网模型(8 台电脑,6 名学生使用),如图 1。

$A_c = \{1, 2, 3, 4, 5, 6, 7, 8\}$; 全部电脑集合

$S_c = \{1, 2, 3, 4, 5, 6\}$; 正常使用的电脑集合

则,可能有故障的电脑集合 $P_c = A_c - S_c = \{7, 8\}$, 则只需检查 7,8 两台电脑。

改进:

$A_c = \{1, 2, 3, 4, 5, 6, 7, 8\}$; 全部电脑集合

$S_{c_{PM}} = \{1, 2, 3, 4, 5, 6\}$; 上午正常使用的电脑集合

$S_{c_{AM}} = \{3, 4, 5, 6, 7, 8\}$; 下午正常使用的电脑集合

则, 正常使用的电脑集合 $S_c = S_{c_{PM}} \cap S_{c_{AM}} = \{1, 2, 3, 4, 5, 6, 7, 8\}$

则 $P_c = A_c - S_c = \varnothing$, 即当天所有电脑都被正常使用, 不需要检查。

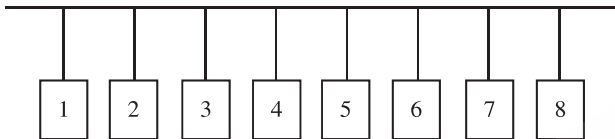


图 1 简化局域网模型

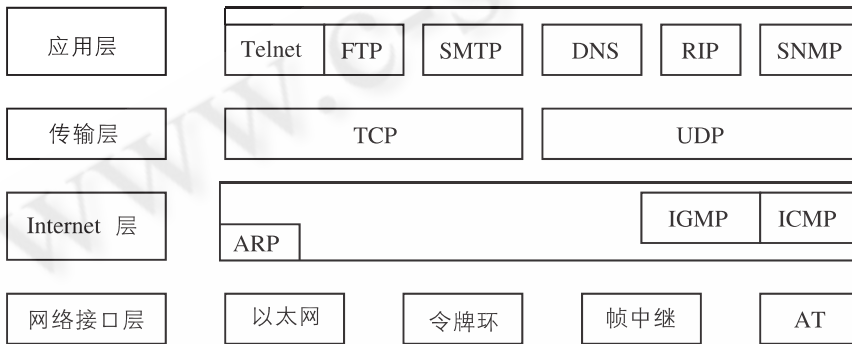


图 2 TCP/IP 模型及协议组

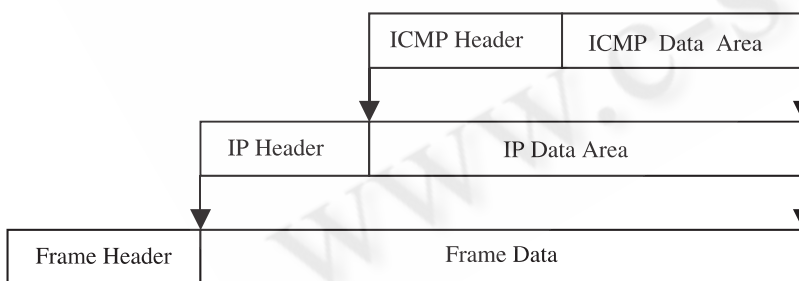


图 3 ICMP 发送时的两层封装

如果某天某一台电脑(假设 8 号)有故障。第二天不可能有人使用 8 号电脑。 $\odot 8 \notin S_c \wedge 8 \in A_c, P_c = A_c - S_c$ 。 $\therefore 8 \in P_c$, 即, P_c (可能有故障的电脑集合)中一定包含 8 号电脑, 所以检查集合 P_c 内的电脑, 有故障电脑被发现, 且最大时间延迟为 1 天。

本人所维护的机房 $|A_c| = 39, |S_c| \approx 35, |P_c| = |A_c| - |S_c| \approx 4$ 。自动检测一次就排除了 35 台正常的电脑, 只检查 4 台电脑就可确定有故障的电脑。用时约是原来的 1/10。

4 局域网计算机状态自动检测方法的实现

4.1 局域网计算机状态自动检测的原理

为了探测一台电脑是否启动及网络是否联通, 这里采用了 TCP/IP 协议簇中的 ICMP (Internet Control Message Protocol, 互联网控制报文协议)。下面对其进行简要介绍。TCP/IP 模型^[2]及协议组, 如图 2。

由图 2 可以看出 ICMP 协议是 Internet 层的一个协议。它和 IP (Internet Protocol) 是互相支持的。IP 有错误消息要发送时, 使用 ICMP 协议。ICMP 要发送报文时, 封装在 IP 协议包中发送。ICMP^[1]协议的封包过程如图 3。

ICMP 定义了 5 类错误报文和 4 类信息型报文。5 类错误报文是: Source Quench (源抑制), Time Exceeded (超时), Destination Unreachable (目的地不可达), Redirect (重定向), Fragmentation Required (请求分段)。4 类信息型报文: Echo Request/Reply (回应请求/应答), Address Mask Request/Reply (地址掩码)。

使用 ICMP 报文测试可达性^[1]。许多工具通过发送探测报文并且等待 ICMP 应答的方式得到互联网信息。Ping 程序是 TCP/IP 使用的最著名的诊断工具。它通过发数据报到指定的目的地并等待回答的方式来测试给定的目的地是否可达。Ping 通过宣告目的地是否应答来报告探测结果。

Ping 使用 ICMP 的 Echo Request/Reply。用户通过给定 IP 地址或远程计算机名称来调用 Ping 程序。Ping 发送一个包含 ICMP 回应请求报文的数据报给目的地, 目的地返回一个回应应答报文。如果没有应答, ping 再发送请求两次。如果没有重发的应答 (或者一个 ICMP 不可达报文到

达), ping 宣告该远程机器不可达。

本文就是采用了该原理,使用 ICMP 的 Echo Request/Reply 探测远程机器是否在线。

ICMP 头结构^[3],如图 4。

类型(8位)	代码(8位)	校验和(16位)
不同的类型或代码有不同的内容		

图 4 ICMP 头结构

BYTE Code; //子代码

WORD CheckSum;

} ICMP_HEADER, *PICMP_HEADER;

5 局域网计算机状态自动检测软件介绍

笔者用 Access 数据库记录局域网计算机状态,用 C++ 语言在 VC++ 6.0 环境下实现上述方法。下面对该软件加以简要介绍。

记录计算机状态用 Access 数据库管理系统,数据库文件名 up.mdb,其中包括表 CompStatus 和表



图 5 计算机故障列表界面

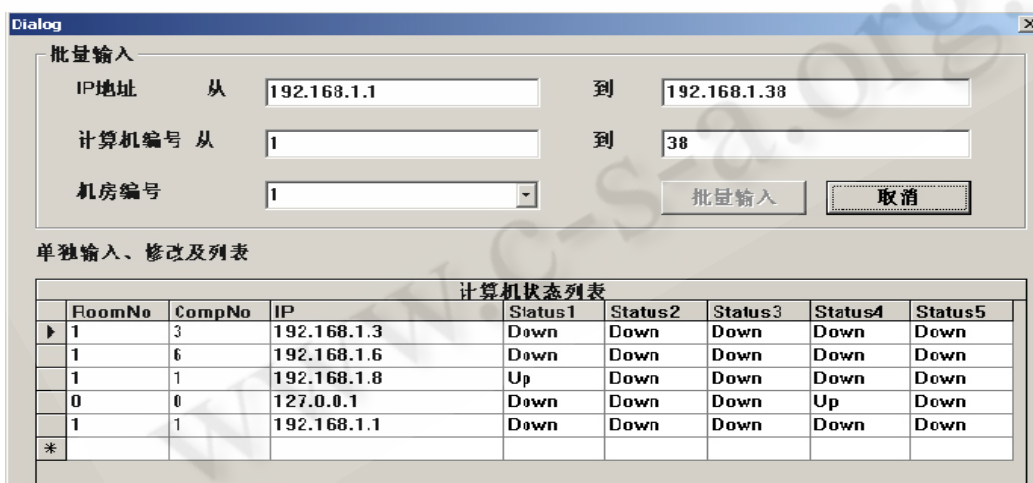


图 6 计算机状态输入界面

类型:8 表示回应请求

0 表示回应应答

C 定义:^[3]

Typedef struct_ICMP_HEADER

{

BYTE Type;

DatePtr。表 CompStatus 用来记录计算机的状态。表 DatePtr 为系统用。表 CompStatus 的字段及意义说明如下:

RoomNo: 机房号

CompNo: 计算机编号

(下转第 85 页)

(上接第 82 页)

IP: 计算机 IP 地址

Status1, Status2, Status3, Status4, Status5: 循环记录计算机状态

软件包括两个: InOut. exe 和 Probe. exe. InOut. exe 用来输入计算机信息和输出计算机状态。Probe. exe 在后台运行, 用来监控时间并定时探测、记录局域网内计算机的状态。

InOut. exe 的界面如图 5、6 所示。

使用说明:

(1) 将 Detect. exe 加入到教师机的“开始”“程序”“启动”, 这样一开机该程序便在后台执行自动探测、记录计算机状态。功能是在上课时间(比如 8:10、10:10、14:40、15:40、20:00)探测联在网上的计算机, 并将其记录在数据库 up. dbf 中。

(2) 不需要在每台电脑中安装客户端软件。

(3) 在数据源(ODBC)中加入用户 DNS 名称为 UP, 其数据库文件为 up. dbf。

(4) 运行 InOut. exe 输入、修改计算机信息, 查看可能有故障的计算机列表。

6 结论

该软件已成功运行在我校教学局域网上, 极大的方便了试验室管理人员的管理与维护, 缩短了维护周期, 提高了工作效率。

参考文献

- 1 Douglas E. Comer, Computer Networks And Internet, 清华大学出版社, 1998. 2。
- 2 石志国、薛为民、江俐 编著, 计算机网络安全教程, 清华大学出版社, 北京交通大学出版社, 2004. 2。
- 3 潘志翔、岑进锋 编著, 黑客攻防编程解析, 机械工业出版社, 2003. 6。