封闭式校园一卡通网络与设备监控系统设计①

Design of Network and Equipment Monitoring System on Closed Campus Card System

何来坤　冯亦山　钟　鸣　徐　渊　(杭州师范大学 电教网络管理中心 浙江 杭州 310036)

摘　要： 由于传统依附于校园网的一卡通系统存在网络的不稳定性和数据的不安全性，本文提出了“封闭式校园一卡通系统”(CCCS)的网络设计理念。文章具体分析了 CCCS 系统网络的设计目标、铺设过程和安全管理等事项，给出与数字化校园网数据对接的方法，以及在 CCCS 系统网络环境中实时监控、排除一卡通设备故障的系统软件设计。该项设计已取得较好实践效果。

关键词： 封闭式校园一卡通系统 CCCS 数字化校园 网络设计 开放与封闭

1　引言

近年来，随着我国高等院校“数字化校园”(Digital Campus)的建设发展，“校园一卡通”也应运而生，成为数字化校园的重要基石。它的稳定性、安全性直接关系到数字化校园的稳定性和安全性[1]。传统的一卡通系统网络平台往往是依附于校园网，在实际应用中，经常会出现系统传输环节的稳定性和安全性问题，一旦校园网络不稳定，就会影响到一卡通运行的稳定，甚至危及数据安全。由于整个校园网络的庞杂和繁复，管理员往往又无法及时判断系统的故障点，造成较严重的后果。我们认为，要从根本上解决这个问题，首先必须转变“数字化校园”的固有观念，校园网并不是越开放越好，而是有的需要开放，有的需要封闭，是开放与封闭的统一。假设把固有的或即将需要建设的校园一卡通系统的网络平台从校园网中剥离出来，使其成为封闭的一卡通专网(如图 1 所示)，就能避免上述存在的问题。从网络架构的角度来说，封闭式结构实现了校园网和“校园一卡通”专网的逻辑隔离，提高了一卡通系统的稳定性和安全性，增强了系统的可维护性和可扩展性，降低了系统的运行管理成本。我们把这种存在于校园内，网络平台与校园网络相对隔离，系统能够独立运营并不受其他网络平台影响的一卡通系统，称为“封闭式校园一卡通系统”(CCCS)。

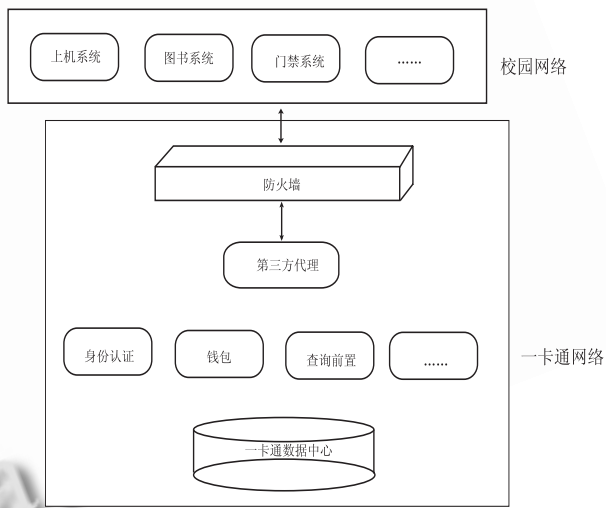

图 1　CCCS 网络结构

2　系统网络设计目标

由于校园一卡通系统在数字化校园中的中所处位置的特殊性，涉及到资金运用、结算和与银行系统的联网，关系到广大教职员工和学生的工作、学习和生活的正常进行，所以稳定性和安全性是两个非常重要的设计环节。

CCCS 系统网络的具体实现目标如下[2]：

(1) 一卡通中心服务器(包括数据中心、身份认证、

① 收稿时间:2008-12-31

流水等)组建独立的局域网络。虽然校园网已经具有相当的网络安全措施，但由于功能繁多，交互频繁，还是存在易受病毒、木马、黑客等攻击可能。因此，系统要求核心服务器所处的网络相对封闭，不与外部系统直接通讯。

(2) 一卡通系统中重要的网关(POS 机)、综合业务机不论场地离中心距离多远，也必须专线专用。

(3) 通过 TCP／IP 控制器(TCP／IP 通讯协议)与管理主机进行通讯。确保在联机状态下的完全实时性要求。

(4) 要求网络能提供全天候的稳定服务，因此核心设备(服务器、网络设备)的选择必须稳定可靠。

3 系统网络铺设过程

CCCS 系统网络设施过程中，系统网络拓扑采用星型结构，各种一卡通网络设备通过中心交换机互连，短距离的网络设备可以采用超五类线直接互联，长距离的设备主要采用光纤通讯介质。在跨校区网络设备互联时，对于只有一根光纤作为实现校区联网业务的通讯媒介，可以用 4 对单芯光纤转换器提供 WDM (Wavelength Division Multiplexing)[3]支持，让 2 个独立的数据传输信道在单芯的标准单模光纤上同时传送与接收资料，这项功能不仅让现有的频宽利用率立即增加 1 倍，更可有效地降低光纤的铺设成本。

4 系统安全管理与数字化校园网数据对接

校园一卡通系统是构建在数字化校园之上的统一身份认证、中央共享数据库、统一信息门户等的基础平台，为了实现这些功能，它在与校园网逻辑隔离的同时，又必须具有相对的开放性，这样才能与学校其它业务管理信息系统紧密结合，实现数据共享和交换，这就是隔离与开放的矛盾[4]。为解决这一矛盾，CCCS 系统中架设有双网卡数据代理服务器，触发器数据交换模式，对数字化校园网和“校园一卡通”专网之间的数据交换采用加密的方式，并在数字化校园网络和“校园一卡通”专网中针对关键服务器制定严格的访问控制策略，禁止非授权用户对这些重要服务器的访问，从而确保“校园一卡通”专网数据的安全。其具体实施安全措施如下：

(1) 在核心交换机上配置访问控制列表(ACL)[5]，例如：

```
ip access-list extend server-protect
permit tcp 192.168.0.0 0.0.0.255 host 192.168.0.20 eq www  //WEB 服务器
permit tcp 192.168.0.0 0.0.0.255 host 192.168.0.13 eq 1521 //数据库服务器
permit tcp 192.168.0.0 0.0.0.255 host 192.168.0.21 eq ftp  //FTP 服务器
……
```

(2) 在与数字化校园网络通讯之间增设防火墙，配置高级访问策略。例如：

```
Quidway(config)#access-list 100 permit tcp 192.168.0.0 0.0.255.255 192.168.99.21 0.0.0.0 eq www  //Web 服务器
Quidway(config)#access-list 100 permit tcp 192.168.0.0 0.0.255.255 192.168.99.15 0.0.0.0 eq 3389  //一卡通数据代理服务器
Quidway(config)#firewall enable  //启用防火墙
……
```

(3) 设置数据异地备份系统。例如：先本机备份，每天定时自动将备份文件通过 FTP 方式上传到异地服务器上。Oracle 数据库中，export 命令将数据库中的数据备份成一个二进制文件，它通常有三种模式：用户模式、表模式和整个数据库模式。如采用用户模式，备份之前，应先建立一个备份目录，以在本机存放备份文件，可建一个/localbak 目录。然后将 School 数据库在用户模式下备份，备份保留周期为一天，具体脚本如下(保留在 exp_school.sh 文件中)：

```
Export EXP_HOME=/localbak          #设置环境变量 EXP_HOME
Export ORACLE_SID=school           #设置环境变量 ORACLE_SID
Exp system/password owner=hsa6 file=$EXP_HOME/SCHOOL$(LC_ALL=C date+%y%m%d).dmp log=$EXP_HOME/SCHOOL$(LC_ALL=C date +%y%m%d).log statistics=none  #备份数据以日期方式命名
……
00 01 * * * ftp -i host2 #每天凌晨 1 点启动远程传输，将文件备份到另一台主机上
```

(4) 单独的 UPS 供电系统。

数据共享盘柜带有 EMC UPS，每个一卡通网关设备各配有山特 1500W UPS。

(5) 一卡通数据中心冗余性。

一卡通数据库服务器利用 Oracle 集群数据库 Oracle RAC(Real Application Cluster)，实现 Linux(Red Hat Enterprise Linux 4)操作系统上的双节点集群[6]。集群环境下实现多机共享数据库，以保证应用的高可用性。同时可以自动实现并行处理及均分负载，还能实现数据库在故障时的容错和无断点恢复。

5 网络设备监控系统

虽然比较依附于校园网的一卡通网络平台，CCCS 网络更稳定，安全性更高，但是任何网络本身都不是绝对可靠的，在 CCCS 系统使用过程中，同样可能会有许多突发事件，导致数据传输失败，网络设备结点故障。为了确保 CCCS 系统正常运营，让管理人员随时掌控运营状况，一旦出现故障，管理人员能及时获取故障点的具体时间地点与故障原因信息，以及时排除险情，因此在 CCCS 系统中设计设备故障报警监控系统是十分必要的。具体实现监控结构如图 2 所示。该系统采用 Delphi+SQLserver 进行开发，C/S 设计模式，系统主要功能：在工作区任一位置中，具备对

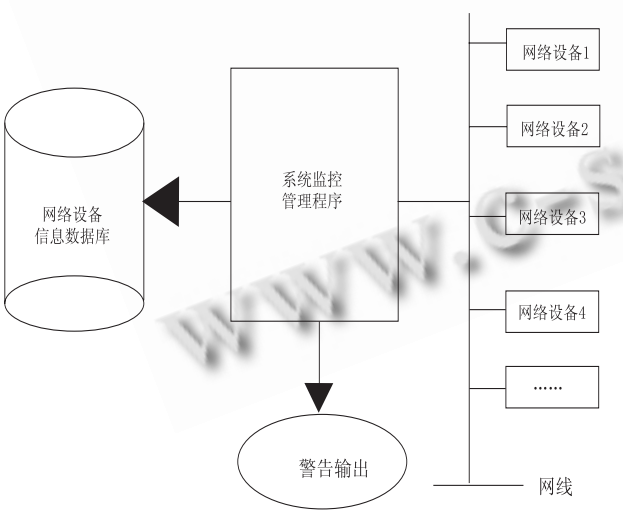

图 2　监控系统结构

网络设备添加，修改，删除功能；设置轮询设备时间；故障报警；日志记录等。系统对各网络设备监测通过 ICMP 协议实现[7]。ICMP(因特网控制报文协议)全称 Internet Control Message Protocol。它是 TCP/IP 协议族的一个子协议，工作在 OSI 的网络层，向数据通讯中的源主机报告错误。实现原理：ICMP 回显请求和 ICMP 回显应答报文是配合工作的。当源主机向目标主机发送了 ICMP 回显请求数据包后，源主机期待着目标主机的回答。目标主机在收到一个 ICMP 回显请求数据包后，它会交换源、目的主机的 IP 地址，然后将收到的 ICMP 回显请求数据包中的数据部分原封不动地封装在自己的 ICMP 回显应答数据包中，然后发回给发送 ICMP 回显请求的一方。如果校验正确，源主机便认为目标主机的回显服务正常，也即网络连接畅通。具体的主要程序代码如下：

```
Function TForm1.pinghost(hst:string): boolean;
  Var
  i : integer;
  begin
  ICMP.Host := hst ; //目标网络设备的名称或 IP 地址
  ICMP.ReceiveTimeout := 1000; //最大等待时间
 Try
      for i:=0 to 3 do    //重复 4 次
      begin
        ICMP.Ping ;
        Application.ProcessMessages ; //延时
  end;
  ......
  procedure TForm1.icmpReply(ASender: TComponent; const AReplyStatus: TReplyStatus);
  begin
      //检测目标主机的回显信息
      If  trim(icmp.Host)=trim(AReplyStatus.FromIpAddress)  then
            pingbz:=true    //回显信息正确
      else
            pingbz:=false;
  end;
```

为使该系统使用更直观化，对监测的网络对象实现了图形化界面。首先创建关于设备的特有类 Teq

=class(TSpeedButton) //利用 SpeedButton 的图形按钮，并定义相关属性如设备描述(Caption)、Ip 地址(ip)、场地(addr)、状态(state)、错误信息等。创建对象，例：neteq:=Teq.Create(self); neteq. addr :=‘XX 校区一期食堂网关’; //对象属性描述……。在对每个工作区中的对象监测时可以使用 pinghost (trim(Teq(Self.Components[I]).ip)) 来判断 ICMP 回显请求报文和回显应答报文是否可达目标设备，如果连续 4 次判断该网络设备 ICMP 回显请求未监听到，表示该网络设备已出现故障，系统则可以通过各种通讯手段(如声音报警、E-mail、手机短信)方式通知管理员进行及时维护。监控系统最终界面如图 3 所示。

图 3 监控系统

6 小结

CCCS 系统对于建设数字化校园网络提供了稳定、安全的共享数据信息的保障。该系统在我校已试行了一年多，通过分析试行阶段的各项数据记录，证明该系统已实现了设计目标，具有在各高校普遍推广的价值。

参考文献

1 华晓鸣.数字化校园一卡通系统的网络安全体系设计.金卡工程, 2007,(9):45－48.

2 尹风雨,孙峥嵘,蒋云霞,卢明.基于数字化校园一卡通系统的安全管理的研究.湘潭师范学院学报(自然科学版), 2007,29(2):73－75.

3 YOOS J B. Wavelength conversion technologies for WDM network applications J. Lightwave Technol., 1996,14(6):955－966.

4 苏文胜,马千军.基于数字化校园的校园一卡通构建.武汉理工大学学报, 2005,27(1):99－101.

5 林辉.利用 Cisco 路由器的 Access-list 提高网络安全.计算机应用, 2001,(2):62－63.

6 付社良,田斌.Oracle RAC 10g 系统高可用性测试及分析.武汉理工大学学报(信息与管理工程版), 2007,29(2):77－78.

7 周斌,李文印.基于 ICMP 的协议的 Intranet 网络监测报警系统的实现.微型电脑应用, 2004,20(2):24－26.