中国地质大学（北京）

信息网络中心文件

信息网络中心　　2010.9.8

中国地质大学（北京）网络与信息安全技术管理措施

随着我校网络与信息化的发展，信息网络中心数据库中存储了越来越多的敏感信息，包括学生信息、教职工信息、工资信息、工科研经费、账号和密码信息，这些信息如果泄露，造成的影响也非常严重。为此，网络与信息安全建设起到至关重要的作用。

信息网络中心是学校的信息技术核心部门，经过多年的建设，从人防、物防、技防等三个方面入手，打造了一个多层次、立体化的校园网安全体系。

参照 TCP/IP 协议的分层思想，我们把基于网络与信息安全技术管理也分为五个层次，即物理层安全、网络层安全、操作系统层安全、应用系统安全和安全管理层等几个方面。

安全体系架构如下图所示：

图 1 网络与信息安全体系

一、物理层安全

物理层安全可分为物理环境安全、线缆安全、网络和主机设备的物理安全等。

1. 环境安全性

环境安全主要指网络设备和服务器所处的机房环境的稳定性。主要包括温度、湿度、电流电压等。

计算机设备尤其是交换机等设备对机房的温度有着较高的要求。温度偏高，易使机器散热不畅，使晶体管的工作参数 产生漂移，影响电路的稳定性和可靠性，严重时还可造成元器件的击穿损坏。

高湿度对网络设备和计算机的影响很大。空气潮湿，易引起设备的金属部件和接插件管部件产生锈蚀，并引起电路板、插接 件和布线的绝缘降低，严重时还可造成电路短路。空气太干燥又容易引起静电效应，威胁通信设备的安全。高湿度对计算机及网络设备的危害是明显的，而低湿度的危害有时更加严重。在低湿状态下，计算机机房中，穿着化纤衣服的工作人员，活动地板以及机壳表面等，都不同程度地积累静电荷。若无有效的措施加以消除，此电荷越积越高，过高的静电电压容易对电子产品造成损害。

此外，高温、高湿、低温干燥等交替变化的环境，由于材料毛细管的呼吸作用，会进一步加速材料的吸潮和腐蚀过程，对计算机设备造成的危害尤为严重。

按照电信机房的要求标准，A 类机房：

正常温、湿度范围：温度 10-25 度，湿度 40%-70%RH

可接受温、湿度范围：温度 10-26 度，湿度 40%-75%RH。

断电及电压引起的问题也是非常严重的问题。当市电发生异常，将造成计算机当机，甚至造成硬件故障，到时维修费将不可预期。其他市电电压过低、过高、突波、噪声等，

均是足以影响设备正常运作的电源品质问题。所以说温度、湿度、电压等一系列物理环境不稳定导致的问题都是归结为物理环境问题。

信息网络中心在318中心机房配备了精密空调，具有恒温恒湿的作用，在中心机房及各楼宇机房都建有温、湿度监控系统，每天值班人员通过登录运维系统就可以查看各个机房的环境情况。

信息网络中心机房在316室配备了独立的UPS室，里面配置了3台40K VA的UPS不间断电源系统分三路向机房供电。机房的每个机柜后面都PDU都连接了两路不同的UPS。服务器的两个冗余电源分别连接到不同的PDU上，这样就保证了每台服务器都不会由于一台UPS故障而导致宕机。

2．线缆安全

通信线缆是信息传输的主要载体，线缆的意外中断、损毁都会导致通信的中断，引发严重的网络故障。

为了保证线缆的安全性，信息网络中心到各个楼宇的都铺设了2路光缆，每路光缆都采用12芯以上光纤，有效地保证了光纤线路的冗余性。光缆的室外部分全部进入到地下管井，防止了意外的刮断和人为破坏。

3．设备物理安全

对服务器和网络设备的直接物理破坏是最致命的。信息网络中心机房及各楼宇机房都安装了防盗门和防盗窗。中心

机房采用门禁系统，具有严格的管理制度，除必须的巡检值班外，大多数操作都是远程完成的。有效防止了闲杂人员对服务器和网络设备的直接接触。保证了设备的物理安全。

二、网络层安全

网络层安全性主要包括网络传输与接入，是传统网络安全中最重要的部分。绝大多数的网络攻击都从扫描 IP 地址与端口和用户接入开始的。

1.网络传输安全

信息网络中心在网络出口部署了两台 Juniper SRX 3600 防火墙，有效地进行了内、外网隔离。Junper SRX 3600 是采用先进的架构，采用电信级硬件平台，通过多内核系统实现用户对安全设备线性处理能力的需求。支持虚拟防火墙技术，支持安全区域间默认访问控制；支持基础、扩展和基于接口的状态检测包过滤技术，支持按照时间段进行过滤；支持对每一个连接状态信息的维护监测并动态地过滤数据包，支持对 FTP、HTTP、SMTP、RTSP、H.323（包括 Q.931，H.245，RTP/RTCP 等）应用层协议的状态监控，支持 TCP/UDP 应用的状态监控。

可以防范多种攻击：包括多种 DoS/DDoS 攻击防范（CC、SYN flood、DNS Query Flood 等）、ARP 欺骗攻击的防范、提供 ARP 主动反向查询、TCP 报文标志位不合法攻击防范、超大 ICMP 报文攻击防范、地址/端口扫描的防范、ICMP 重定

向或不可达报文控制功能、Tracert 报文控制功能、带路由记录选项 IP 报文控制功能；静态和动态黑名单功能；

两台防火墙每个上面虚拟了 4 个逻辑防火墙，分别对应着 4 条出口线路。两台防火墙同时互为备份，消除了单点故障。

2. 网络接入安全

（1）IP 地址实名制与 MAC 地址绑定

校园网所有 IP 地址实行实名制，IP 地址的分配和管理由信息网络中心负责，并与用户电脑 MAC 地址绑定。

用户首次申请地址时，登录 IP 地址管理系统 http://ip.cugb.edu.cn,输入身份证号和学号，进行实名认证成功后，方能进入系统。

图 2MAC 注册自助登录

在地址管理系统中，用户输入上网电脑 MAC 地址，核对个人信息无误后，提交 IP 申请。经后台审批后，即可获得

IP 地址。

图 3MAC 注册表单，其中“学号/工号”由数字校园规则生成

（2）无线接入

中国地质大学（北京）无线网由中国地质大学和中国电信合作建立。无线网络覆盖面广，采用地质大学和中国电信双 SSID：中国电信的“ChinaNet”和中国地质大学（北京）的校园无线网“CugbNet”。校园无线网由信息网络中心统一管理。

图 4 校园网无线用户选择“CugbNet”

用户在使用无线网络时，选择“CugbNet”自动连接到校园无线网络。连接后，自动分配 IP 地址，可以访问内网资源。

如需登录外部网站，系统自动跳转到认证页面进行网络准入认证。只有通过了网关系统的准入认证，才可以真正访问互联网资源。

图 5 校园网无线用户访问外网网关认证

（3）VPN 系统

为了满足校外师生访问内网资源的需要，网络中心部署了 VPN 系统。VPN 即虚拟专用网，是为通过公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。使用这条隧道可以对数据进行安全加密以达到安全使用互联网的目的。VPN 系统是对校园内部网络的有效扩展，可以具体解决住在校外用户、出差用户、野外实习用户等查看校内资料的问题。VPN 系统采用专人管理，所有认证账号来自于校园网统一认证系统。

（4）用户统一身份认证及密码安全策略

我校师生依据数字校园统一编码生成用户 ID，由统一身

份认证平台管理用户访问信息化应用系统。统一身份认证平台主要包括以下方面：

1）目录服务：基于开源的 OpenDJ 目录服务、支持 X.509 协议、提供细粒度的资源访问控制列表（ACL）、实现目录对象与数据同步复制；平台提供了外部数据源向统一身份认证平台同步身份数据的功能，并可灵活设置数据同步策略；目录服务定义了符合学校特点的身份数据规范，实现了用户信息规范命名、统一集中存储，用户 ID 全局唯一。

2）统一身份管理：包含身份管理、身份信息同步、身份状态的转变。平台提供了创建用户、用户组，查询、修改用户及用户组详细信息功能，能够实现用户类型管理、日志管理、配置管理和修改账号密码等功能；能够记录用户登录数字校园应用访问日志，实现用户操审计和追溯。

3）统一身份认证：利用 SSO 及 CAS 技术将众多应用系统集成到信息门户平台中，通过平台提供的统一认证服务，满足学校业务系统多元化特点，实现一次登录即可访问数字校园中各应用系统相应权限内的资源。

4）用户密码策略：用户密码 MD5 加密，密码复杂度 8 位（数字+字母混合编码）、

5）黑名单：目录服务中设置黑名单功能，进入黑名单的用户登录各种系统均无效。用户统一身份认证系统架构如下图所示。

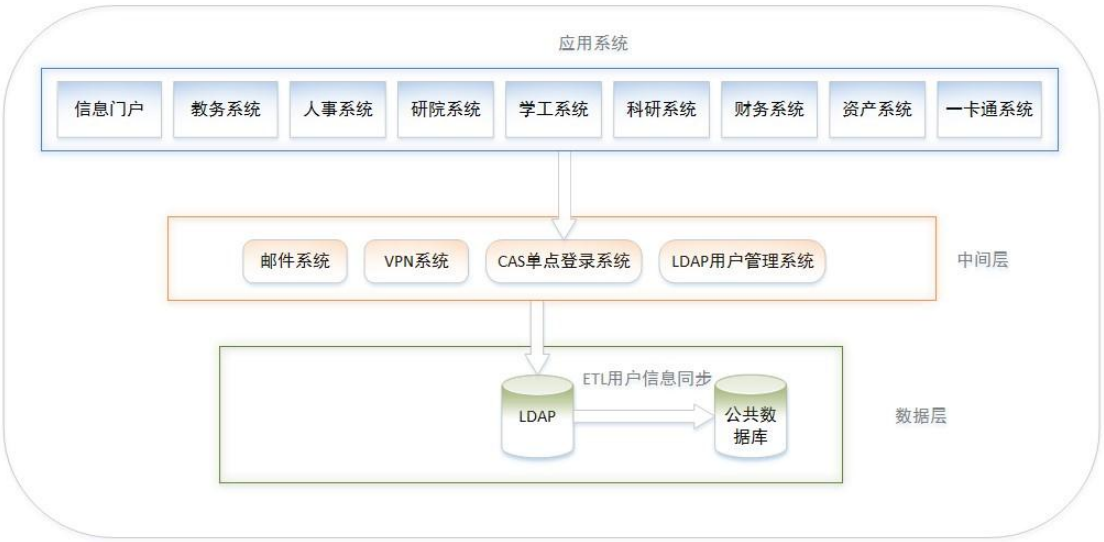


图 6 统一身份认证系统

三、系统安全

所有的软件和应用都是部署在操作系统之上的，操作系统自身的漏洞和脆弱性将给业务系统带来致命的影响。所谓操作系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。无论是 Microsoft 的 Windows 或者其它任何 Linux/UNIX 操作系统，都不是天生安全的。没有完全安全的操作系统。不同的用户应从不同的方面对其业务作详尽的分析，选择安全性尽可能高的操作系统。而且使用前要对操作系统进行安全配置。出于以上的认识，信息网络中心对于操作系统安全从三个方面采取了措施：

1.操作系统安全

信息网络中心的服务器大多采用稳定性和安全性较高的 Linux 操作系统，每个系统正式部署前卸载或关闭不必要的网络服务，设置高安全级别的管理密码。及时安装补丁程

序并升级新版本。

2.虚拟化技术

信息网络中心部署了由八台 DELL R720 高性能物理服务器组成的服务器虚拟化系统。服务器虚拟化系统对操作系统和应用进行抽象化，使其与物理硬件分离，可以获得一个更加经济高效、敏捷和简化的服务器环境。借助服务器虚拟化，多个操作系统能够以虚拟机方式运行在一个物理服务器上，每个虚拟机均可访问底层服务器计算资源。增强了业务连续性和灾难恢复能力。

服务器虚拟化的一大功能是支持将运行中的虚拟机从一个主机迁移到另一个主机上，而且这个过程中不会出现宕机事件，这样就有效防止了操作系统故障给业务系统带来的服务中断。

3.双机热备或负载均衡模式

对一些重要的系统应用，比如数字校园数据库系统，校园网计费认证系统等不能间断的系统，如果操作系统出现宕机或者崩溃等极端情况会给业务代来不可弥补的损失。

信息网络中心的数字校园 Oracle 数据库系统采用 RAC 的双机热备方式，即两台主机的进程及内容实时保持同步，并具有负载均衡关系，当一台主机出现故障或 Oracle 进程宕机，RAC 会自动漂移到另一台主机或 Oracle 进程，RAC 模式极大地提高了系统的可靠性。

邮件系统采用了服务器负载均衡方式，两台前端服务器安装所有前端模块，对用户提供 POP3、Smtp、Webmail、Imap 等服务。服务器通过 F5 设备进行负载均衡。其中一台发生操作系统级别的故障，不会影响到整个邮件系统的服务。如下图所示。

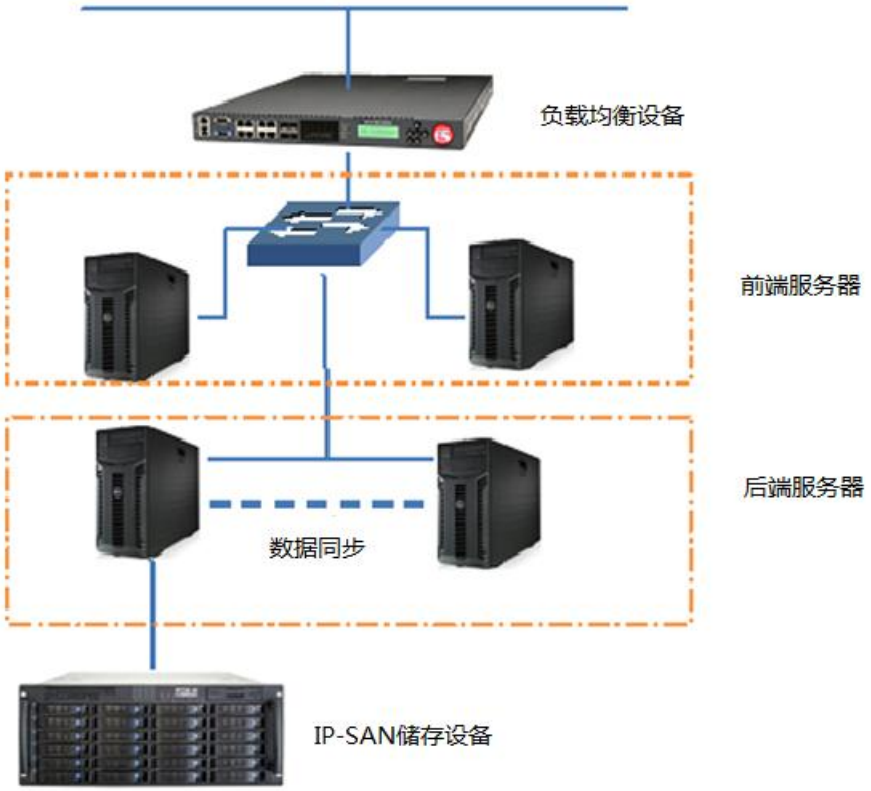


图 7 虚拟化系统架构

4.数据库安全措施

信息网络中心的数字校园等应用系统数据库主要采用 Oracle，数据库的备份恢复是保证数据安全性的重要手段。

数据库备份最基础的工作是每天凌晨以 Oracle Dump 方式自动备份在本地数据库服务器上。

利用数据备份软件 Atempo TimeNavigator 的备份复制

功能每天自动将本地数据库备份文件复制到到备份服务器的虚拟磁带库上。

利用数据备份软件 Atempo TimeNavigator 的备份复制功能每天自动将本地数据库服务器上备份的 dmp 文件每天自动复制到教四楼备份服务器上。

一旦发生数据库崩溃或数据库遭受攻击，数据库系统管理员（DBA）按照下述步骤行数据恢复：

（1）首先从本地数据库服务器上取出最新备份，检查备份文件是否损坏，如果文件完好，则使用此文件进行数据恢复。

（2）如果本地数据库服务器上的备份文件已损坏，则取出备份服务器虚拟带库上的备份文件，检查备份文件是否损坏，如果文件完好，则使用此文件进行数据恢复。

（3）如果备份服务器虚拟磁带库上的备份文件也损坏，则利用异地教四楼备份服务器上的备份文件恢复数据。

（4）如果所有备份均无法恢复，应立即向有关厂商请求紧急支援。

参见《中国地质大学（北京）数据备份安全措施》

四、应用系统安全

应用系统层是直接面对用户提供服务的层面，近年来网络攻击的重点已经从传统的网络层攻击转移到对应用系统的攻击，比如近年常见的 WEB 攻击、Struts2 漏洞攻击，都

属于应用层安全的范畴。以web攻击为例，在Web 2.0的技术趋势下，各网站不断增加网站上的功能，尤其是增加互动，以提供更好的用户体验，极大的流行使得 75%以上的网络攻击都瞄准了 Web，而随着 Web 应用类型的丰富，Web 攻击也丰富起来，遭受Web攻击会使学校网络安全面临的巨大风险。

网站自身及客户的数据泄露风险巨大，网站的声誉极易受损；网站可用性难以保障，业务中断带来的损失巨大；业务的复杂、多样化，使得安全策略配置困难，难以贴合业务环境；网站管理员也面临着同样的挑战：用“改代码”的方法修补网站漏洞需要付出过高的代价，人工查找和分析漏洞的时间周期过长等等。传统的网络防火墙不能检测到应用攻击，原因是它们攻击的大多是合法应用程序的开放端口，虽然网络防火墙检查端口和packet headers，但是，它们并不能核查应用程序和应用程序数据，它们可以在通过开放防火墙端口时，不知不觉地隐藏恶意活动。针对日益严重的应用层安全威胁，信息网络中心采取了部署Web应用漏洞扫描系统、反垃圾邮件和反病毒邮件系统、Web 防火墙系统等保障应用层安全。

1.Web应用漏洞扫描系统。

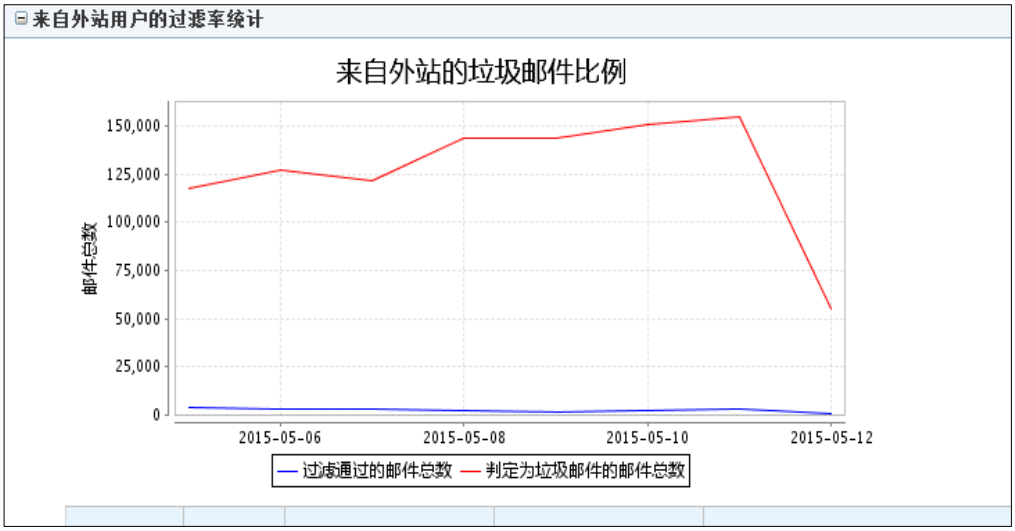
信息网络中心部署了绿盟应用漏洞扫描系统，该系统采用高效稳定的扫描引擎，基于嵌入式系统平台，通过内核级优化，运用智能页面爬取、资源动态调节、代理缓存机制和

实时任务调度等技术，实现了对大规模网站的快速、稳定的扫描，提供了全面的 Web 应用安全检测。采用多视角风险评估模型，同时提供了安全评估和风险自评两种模式，既可以周期性的进行全面安全检测，还可以结合实际业务系统进行深入的安全评估。专家级统计分析报告，融入漏洞修补流程和漏洞精确定位技术，既可以展示各站点的整体风险等级和对比风险情况，还可以直观、便捷的查看每个漏洞的详细信息及修补建议，很好的帮助用户分步骤的修补漏洞以及验证修补效果。

图 8 漏洞扫描系统

2.垃圾邮件和病毒邮件过滤

信息网络中心采用 Coremail 反垃圾邮件和反病毒邮件系统，帮助邮件系统抵御最新的垃圾邮件、病毒邮件、欺诈性邮件、钓鱼邮件、间谍程序邮件等各类邮件威胁。提供强大、易用、高性价比的反垃圾及病毒邮件解决方案，满足当前复杂的互联网环境下垃圾邮件防护需求。每天垃圾邮件的过滤率在 98%以上。



域名	邮件数里	流里	病毒邮件数	发现病毒个数
artistshousemusic.com	5	1496103	5	5
aol.com	13	7196754	4	4
cugb.edu.cn	5756	5214564830	3	3
sina.com	148	502110106	2	2
druckerei-harder.de	2	1237011	2	2
gov.us	0	0	1	1
honjij.asia	0	0	0	0
howur.biz	0	0	0	0

图 9 邮件过滤系统分析

五、安全管理

管理是网络与信息安全最直接最重要部分。责权不明，安全管理队伍及制度不健全及缺乏可操作性等都可能引起管理安全的风险。当网络出现攻击行为或网络受到其它一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可

控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。人员和技术的结合是做好安全管理的关键。

1. 网络与信息安全队伍

我校已经建立了网络与信息安全队伍，队伍成员分工明确，责任到人。参加《中国地质大学（北京）校园网络管理小组及职责》、《中国地质大学（北京）信息安全工作领导小组》。

2. 网络准入用户实名制

校园网实行用户实名准入制，每个用户入网前都要在 IP 地址管理系统中注册电脑网卡地址，核对姓名、住址、电话等信息。管理员分配 IP 地址后，将 IP 与网卡地址进行绑定，实现了用户和 IP 的一一对应关系。如果用户访问外网，必须登录网关，验证身份，然后才可以访问外网。实现了用户和访问地址的对应关系。

编辑	选择	工号/学号	姓名	部门	楼宇	楼层	房间号	余额	状态	二层交换机IP	端口	IP	MAC	绑定	禁用	注册时间
		2014010040	刘志坤	地信学院	逸夫实验楼	2	201	23.9	A			121.194.88.193	0014.4FEA.A9A4	是	否	2015-05-11
		1012142223	马诗舟	土科学院	学19楼	4	中403	20	A			115.25.73.93	68F7.2844.D282	是	否	2015-05-11
		1010143109	李崇	地信学院	学19楼	3	东315	40	A			115.25.74.192	ACB5.7DFB.A35A	是	否	2015-05-11
		2005011938	敖卫华		测试楼	1	101	0	L	192.168.6.68		202.204.106.67	0001.6C4E.9370	是	否	2015-05-11
		201410040	刘志坤	地信学院	逸夫实验楼	2	201					121.194.88.233	0CC4.7A12.79AC	是	否	2015-05-11
		1010131232	马得文	地信学院	学18楼	6	617	20	A				68F7.283F.95D4	否	否	2015-05-10
		1002131309	闫百武	工程学院	学18楼	2	216	30	A			219.225.53.107	201A.06C7.5B30	是	否	2015-05-10
		2014010021	刘广耀	研生院	逸夫实验楼	3	312	0	L			121.194.88.93	EC26.CA99.3CDC	是	否	2015-05-08
		3003140018	张茜	材料学院	学17楼	11	1107	10	A			121.194.81.20	A820.6625.BCEb	是	否	2015-05-08
		2013010050	陶树	能源学院	测试楼	4	420	0	L	192.168.6.67		202.204.106.167	0857.0060.E3B8	是	否	2015-05-08
		2002011487	张洁	材料学院	测试楼	1	120	0	L			202.204.106.76	EC26.CA79.9631	是	否	2015-05-08
		1004112213	符钧阮	信工学院	学19楼	7	中716	30	A			219.225.63.122	B870.F431.3458	是	否	2015-05-08
		1004112131	徐亮	信工学院	学19楼	7	中716	50	A			219.225.63.28	206A.8A6D.C59F	是	否	2015-05-08
			管科rt	文管学院	教4	3	313			192.168.1.123		202.204.96.85	BCD1.773D.45D3	是	否	2015-05-07
		1002131308	刘昊	工程学院	学18楼	2	216	20	A			219.225.52.21	206A.8AB2.2550	是	否	2015-05-06

图 10 IP 地址管理系统用户信息列表

3. 运维系统

信息网络中心为网管及值班人员提供专业的运维系统，网管和值班人员可以远程查看机房的温、湿度，网络拓扑和各种阀值报警，及时发现故障隐患并快速反应处理。

图 11 中心机房环境监控

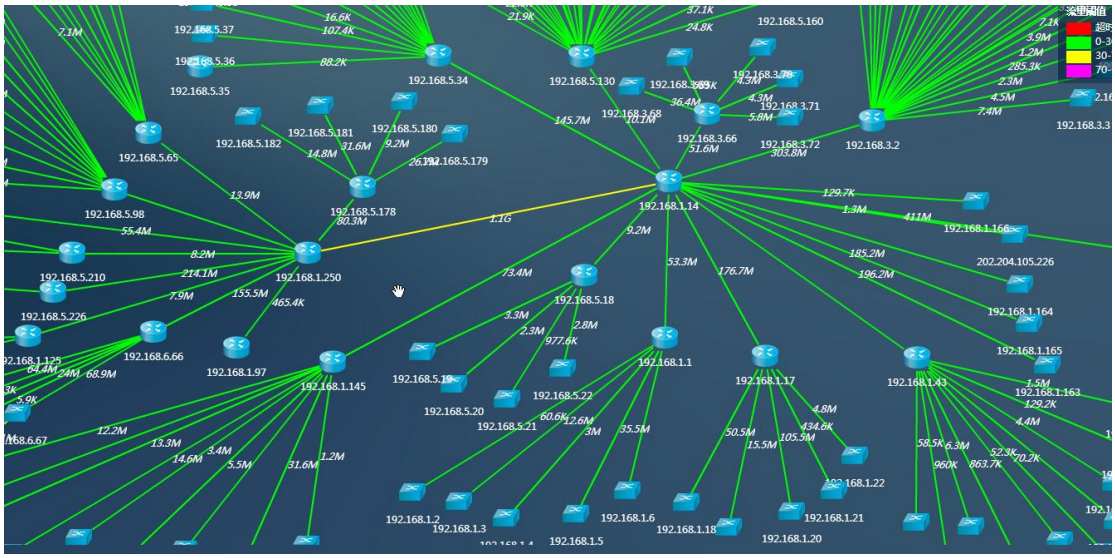


图 12 网络交换机流量图

4. 网络日志系统

网络中心购买了绿盟公司网络日志系统，通过此系统可以根据公安机关以及宣传部门的需要进行日志反查。同时制

定了严格的反查制度，有效地保护了用户的隐私。

	时间	上报设备	事件类型	用户	源IP	目的IP	摘要信息
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		121.194.92.198(北京市)	163.177.68.178(广东省)	关键字: 站点:v.gdt.qq.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		219.225.40.208(北京市)	113.105.143.246(广东省)	关键字: 站点:cdntel.115.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		202.204.107.224(北京市)	140.205.164.98(北京市)	关键字: 站点:detail.tmall.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		219.225.63.19(北京市)	123.126.32.32(北京市)	关键字: 站点:123.126.32.32:5540
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		192.168.194.236	211.152.49.184(上海市)	关键字: 站点:bea.wufazhuce.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		219.225.48.150(北京市)	60.210.11.62(山东省)	关键字: 站点:www.douyutv.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		192.168.194.169	121.43.78.39(北京市)	关键字: 站点:crm.qufenqi.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		219.225.37.54(北京市)	115.25.217.12(北京市)	关键字: 站点:hot.vrs.sohu.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		219.225.50.241(北京市)	163.177.65.252(广东省)	关键字: 站点:interface.finance.qq.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		202.204.106.212(北京市)	123.126.104.8(北京市)	关键字: 站点:hq.stock.sohu.com
	2015-05-12 09:57:57	202.204.105.35 (SAS)	网页浏览		121.194.81.38(北京市)	211.90.30.31(北京市)	关键字:

图 13 日志分析

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是制定健全的管理制度和严格管理相结合。保障网络的安全运行，使其成为一个具有良好的安全性、可扩充性和易管理性的信息网络便成为了首要任务。一旦上述的安全隐患成为事实，所造成的对整个网络的损失都是难以估计的。因此，网络的安全建设是校园网建设过程中重要的一环。

5. 网站安全监测系统

网络中心购买了绿盟公司“网站安全监测系统”，该系统能够根据站点管理者的监管要求，通过对目标站点进行不间断的页面爬取、分析、匹配，为客户的互联网网站提供远程安全监测、安全检查、实时告警，是构建完善的网站安全体系的最好补充。