构建安全和谐的信息化校园

—复旦大学校园网安全与保障体系

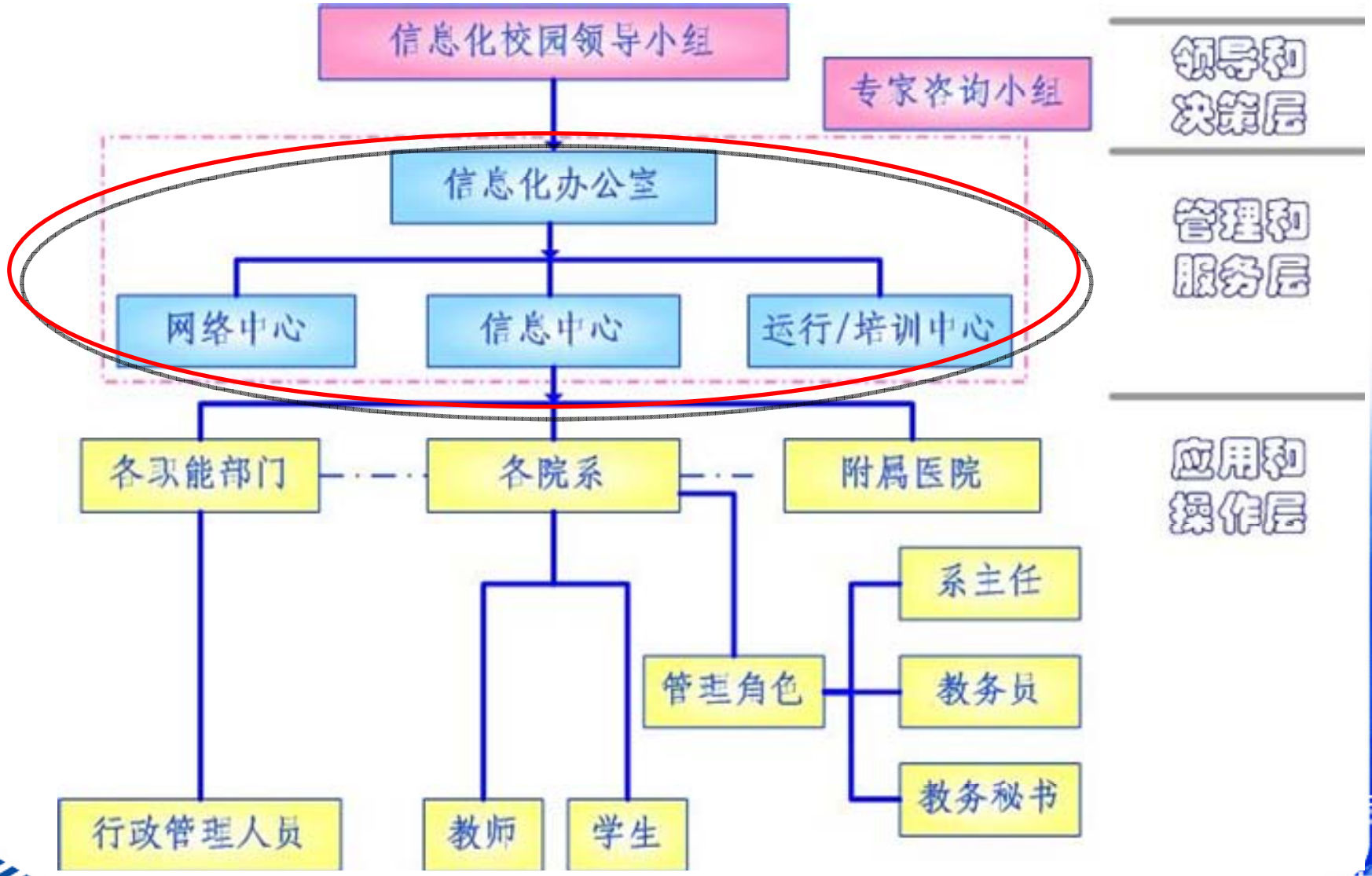
闫　华

2009年5月27日

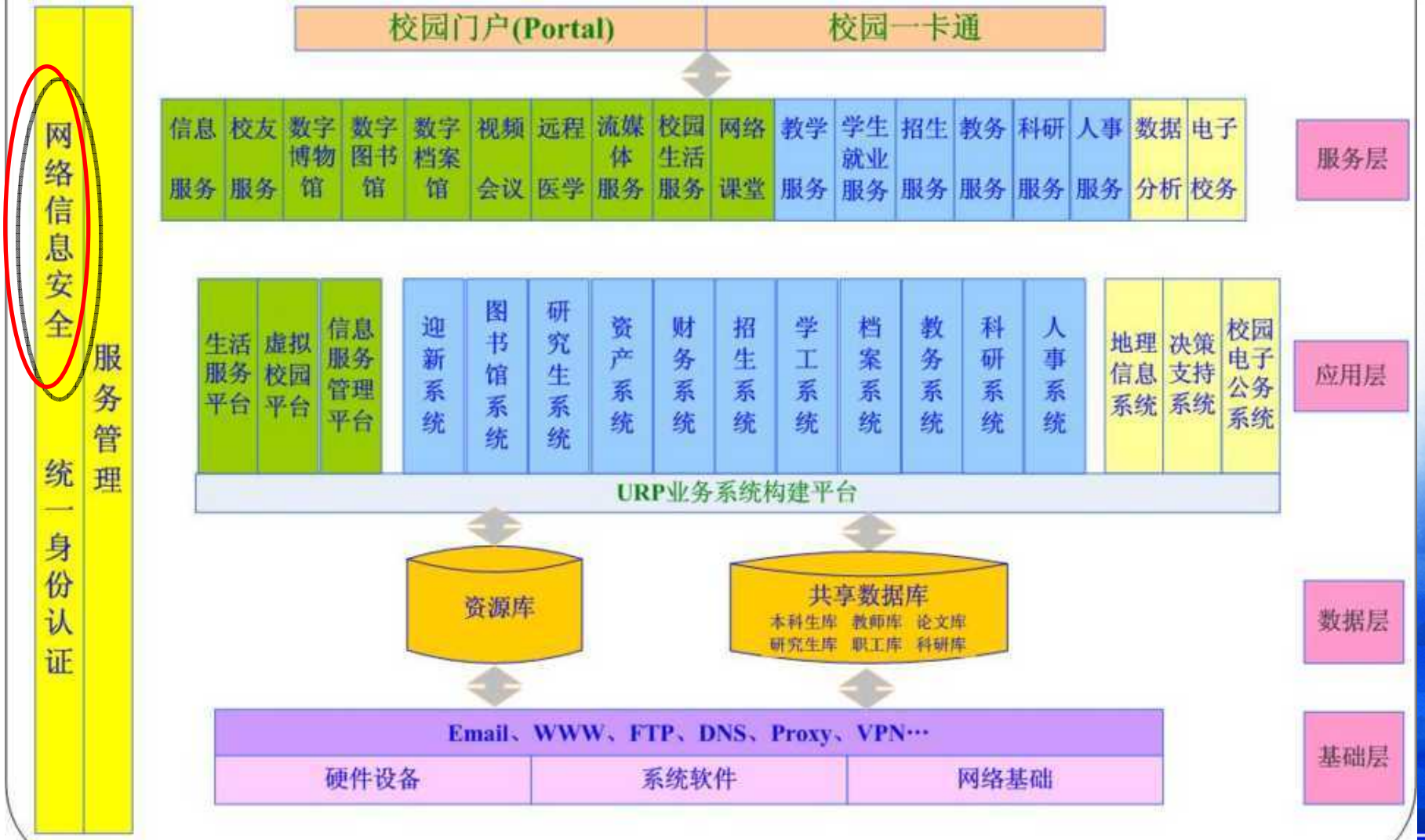
复旦大学信息化办公室
Informatization office of Fudan University

1. 复旦大学信息化校园建设
2. 安全：面临的挑战
3. 复旦信息化校园安全保障体系

组织机构落实

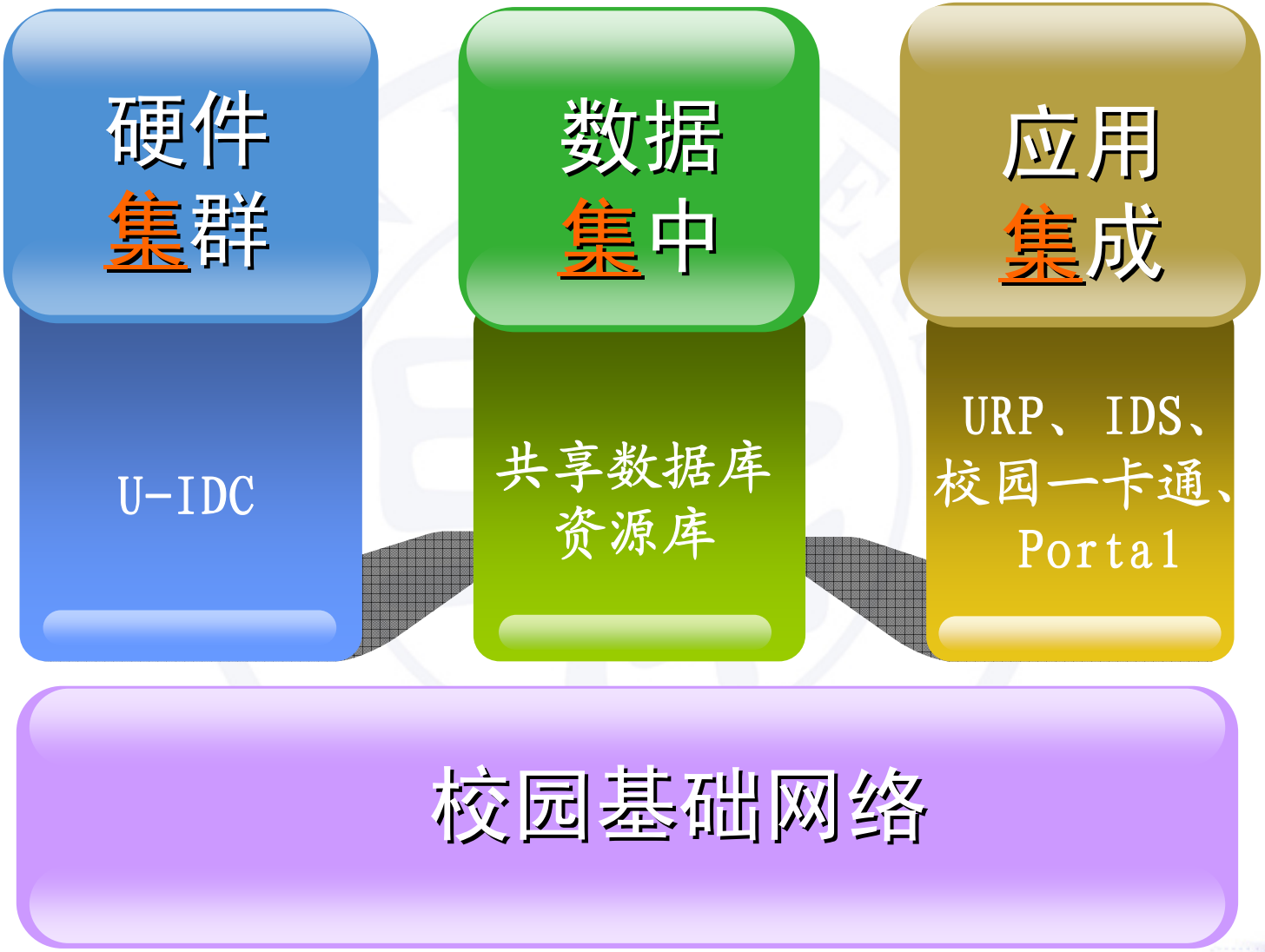

信息化校园领导小组
专家咨询小组
信息化办公室
网络中心
信息中心
运行/培训中心
各职能部门
各院系
附属医院
系主任
管理角色
教务员
教务秘书
行政管理人员
教师
学生
领导和决策层
管理和服务层
应用和操作层

建设架构



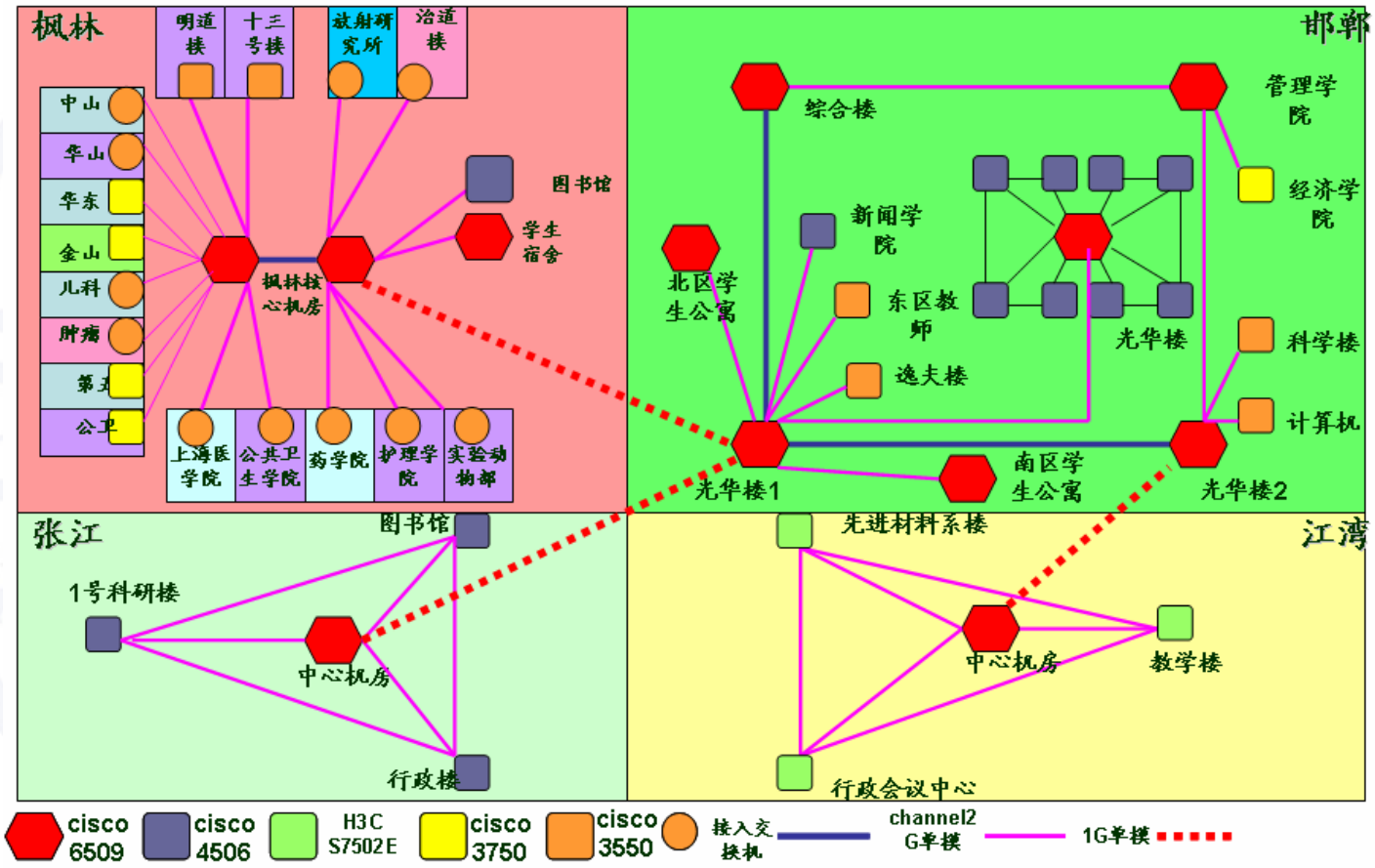
- 单接触点、高度集成、提供个性化服务的校园信息门户(UIP--University Information Portal)
- 强调管理流程集成和数据信息实时性的校园资源规划(URP--University Resource Planning)

复旦校园信息化建设

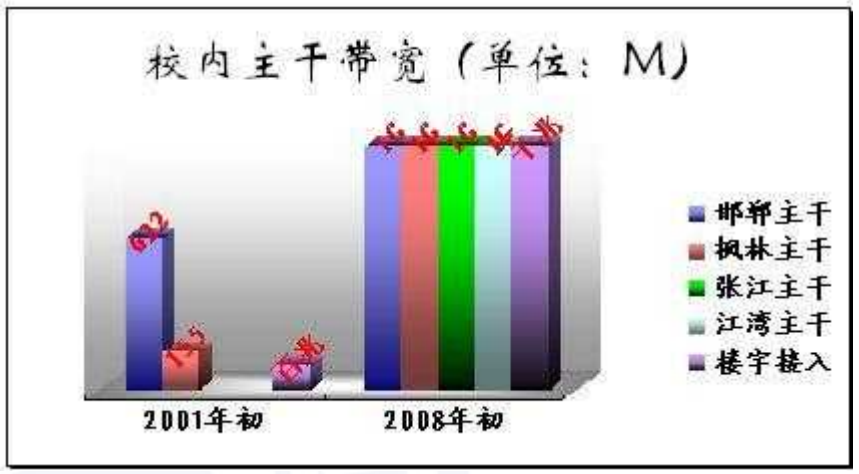


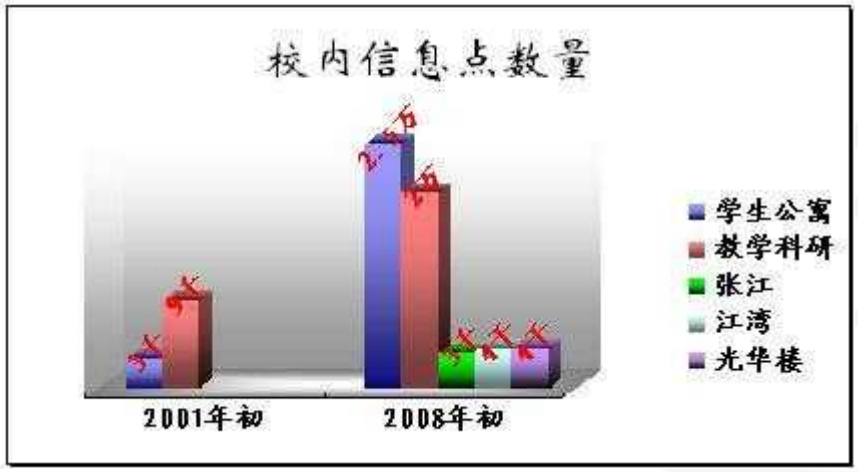
建设成就：校园网

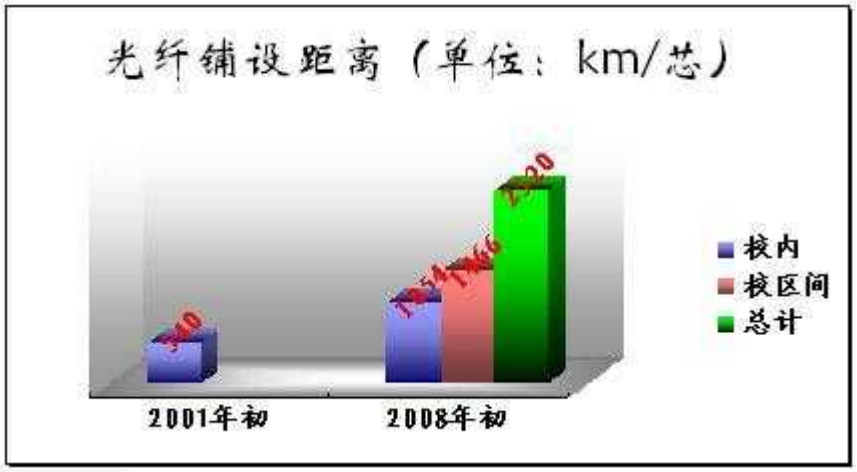
“一体两翼”，跨越整个上海地区的四大校区（邯郸、枫林、张江、江湾），并以此为汇聚接入10所附属医院的局域网，结合IPv4/IPv6、有线无线形成“新一代校园城域网”



网络建设统计数据







E-campus

复旦大学信息化校园安全管理的特点

- 校园网速度快、规模大
- 校园网环境开放，用户活跃
- 信息化校园应用精彩纷呈
- 信息化校园数字资源相对集中
- 计算机系统管理方式复杂多样
- 校园信息化人力和资金投入有限

1. 复旦大学信息化校园建设
2. 安全：面临的挑战
3. 构建安全和谐复旦信息化校园

E-campus

校园网的安全威胁

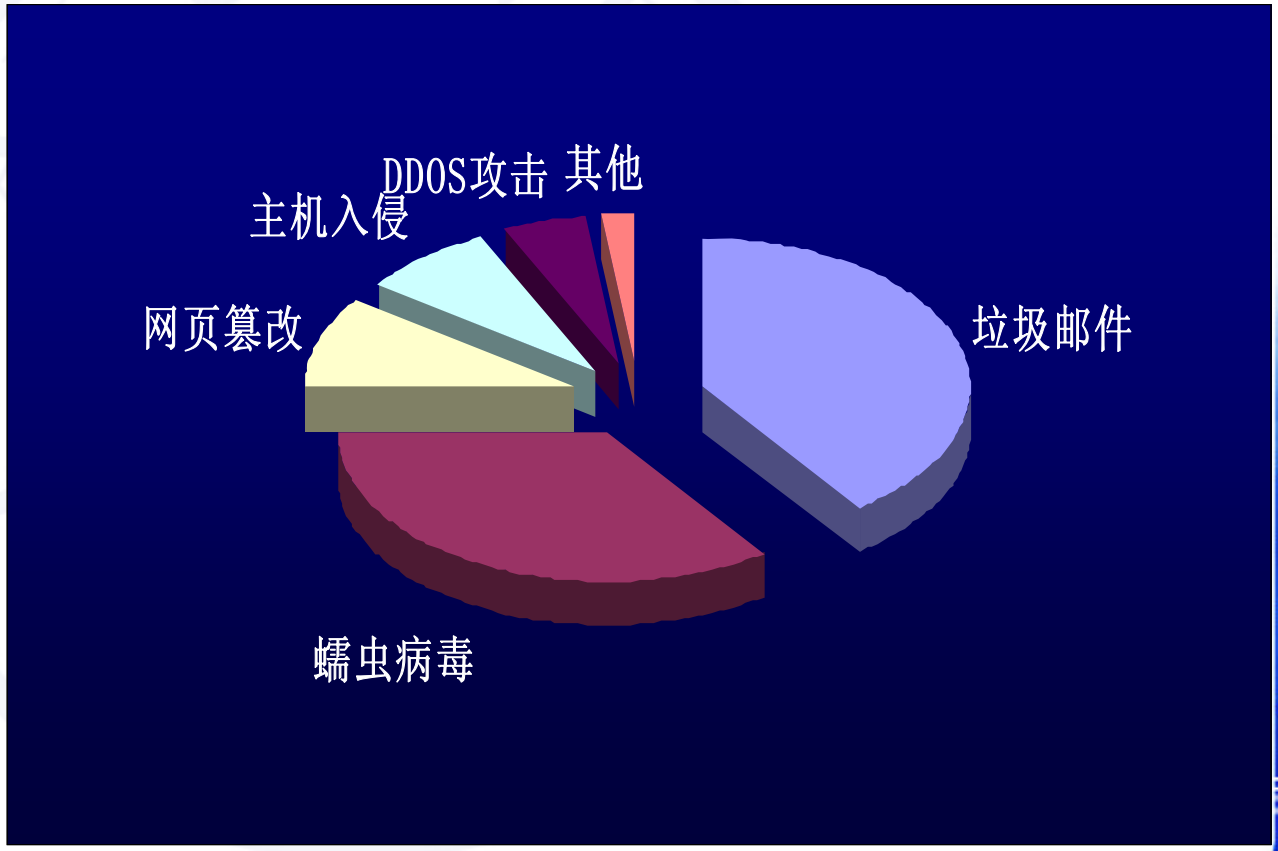
- 随着信息化的发展,校园网络环境变得越来越好
  - 人均信息点占有率>1
  - 大面积无线覆盖
  - 网络化学习工作方式和文化生活
    - Email、 URP 、OA办公自动化、数字档案馆、虚拟校园、资产管理、财务、科研、WebPage...
    - BBS、流媒体平台、高清晰点播、P2P电视、IM即时通信、软件下载、联机游戏...
  - 信息环境的改变导致用户量的剧增，安全问题浮出水面

安全管理的难题

- 安全管理是ITIL的核心
  - 服务器与应用系统安全管理
  - 信息安全管理
  - 客户端安全管理
- 客户端安全管理一直徘徊在比较低的层次
- 客户端安全管理缺乏可操作的安全政策是问题的关键

复旦大学安全事件投诉率

- 1. 垃圾邮件
- 2. 蠕虫病毒
- 3. 网页篡改
- 4. 主机入侵
- 5. DDOS攻击
- 6. 其他



校园网安全事件分类

针对网络和服务器

- 垃圾邮件
- 蠕虫病毒
- 网页篡改
- DDOS攻击
- 局域网ARP欺骗
- 网络扫描

针对个人用户

- 主机入侵
- 木马
- 宏病毒
- 帐号、权限盗用
- 弱口令

1. 复旦大学信息化校园建设
2. 安全：面临的挑战
3. 复旦信息化校园安全保障体系

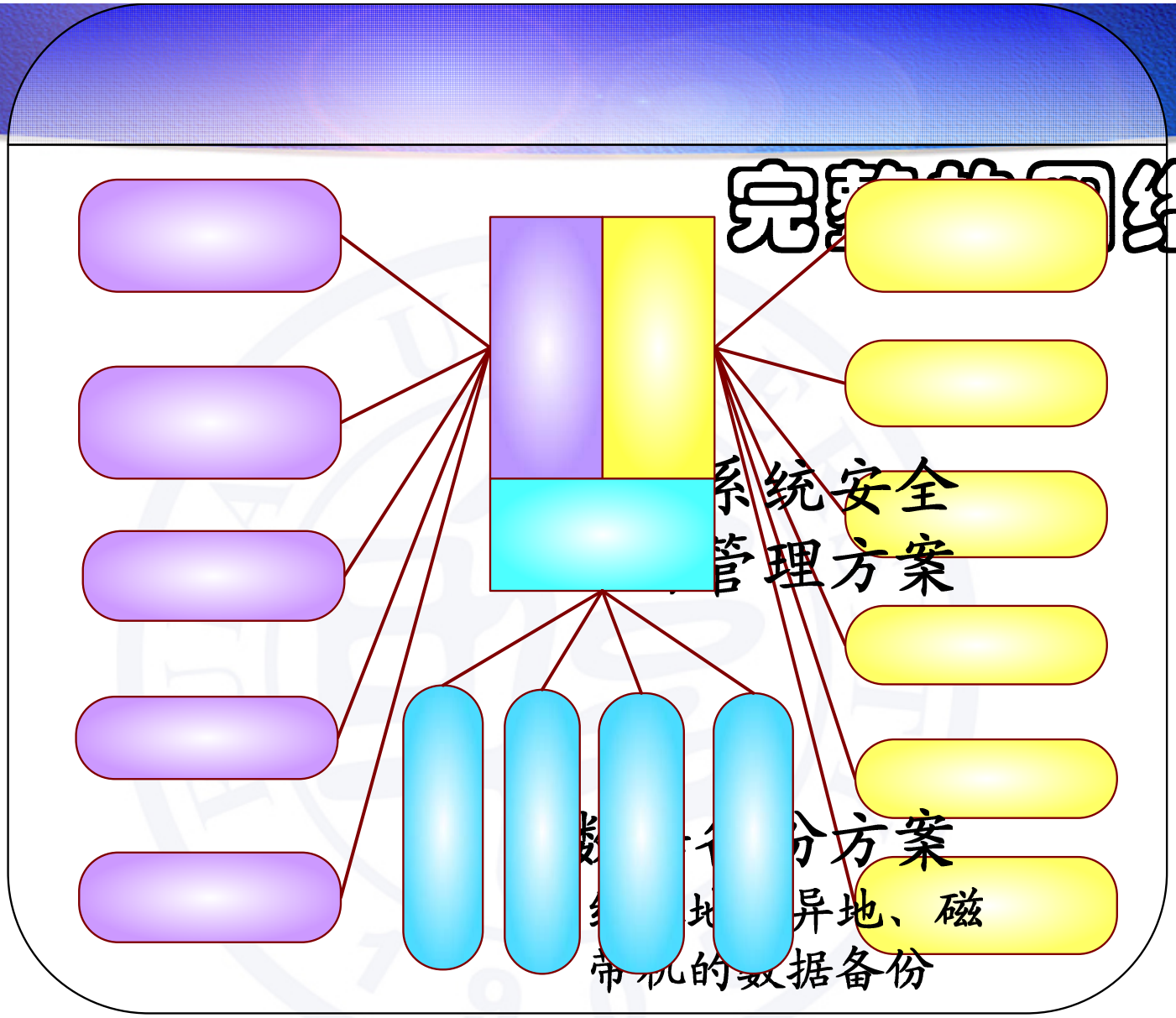
校园网安全工作的目标

安全状态及漏洞评估
安全信息管理预警
异常流量预警

终端安全防护
网络自身安全防护
垃圾邮件防护
应用安全防护
内网安全防护

安全管理体系
安全信息管理
设备及配置管理
安全认证管理

DDoS攻击响应
病毒蠕虫泛滥响应
安全应急响应
24×7客户支持响应



规范管理制度

健全保

根据实际情况，自主进行一些安全方面的实践工作

应急管理流程

安全工作组

- 安全组的组成：
  - 安全领导小组由信息办主任、副主任、各中心主任组成。
  - 安全工作小组由信息办从各中心抽调对网络、信息系统安全技术比较精通的技术骨干7人组成安全工作虚拟团队。

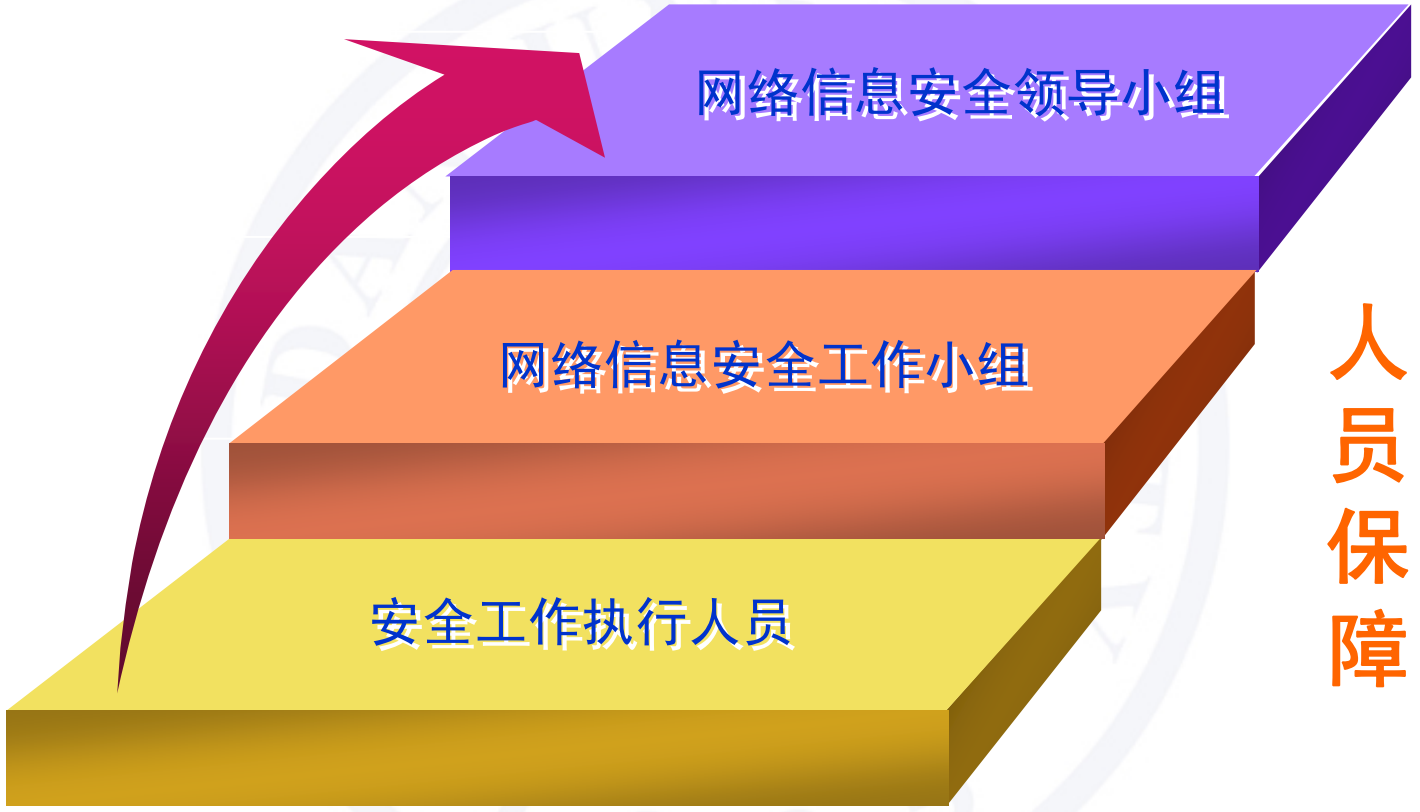
安全领导小组职责

- 把握信息安全的管理方向，制定并发布信息安全规划；
- 参与信息安全方案的制定和评审，对方案的发布执行进行确认；
- 强化及宣传信息安全意识，使信息办每位成员意识到信息安全的重要性，并按安全规范进行工作；
- 对于安全执行小组上报的问题，及时做出决策并确定总体解决方案。

安全工作小组职责

- 按照信息办的有关信息安全方案，定期对信息安全进行检查，并将结果上报安全领导小组
- 定期将信息安全管理与执行情况形成文档，提交安全领导小组审查，并备案;
- 监督并指导信息办成员按安全规范开展工作，保证安全工作的有效执行;
- 小组内部定期组织安全会议，沟通并解决安全执行工作中的问题，会议结论上报安全领导小组;
- 对于新发现的信息安全隐患，且现有管理方案中不涉及，应及时以书面形式上报安全领导小组。

安全工作组架构



人员保障

安全工作的执行由3个中心共同完成

健全保障体系

信息办

- ❑安全方案制定与更新
  - 信息办安全方案
  - 各应用系统安全技术方案
  - 安全方案的更新与升级

网络中心

- ❑防病毒及攻击安全
  - 防火墙设置
  - 杀毒软件设置
  - 更新设置
- ❑网络及服务器安全
  - 网络安全
  - 操作系统安全
  - 服务器安全

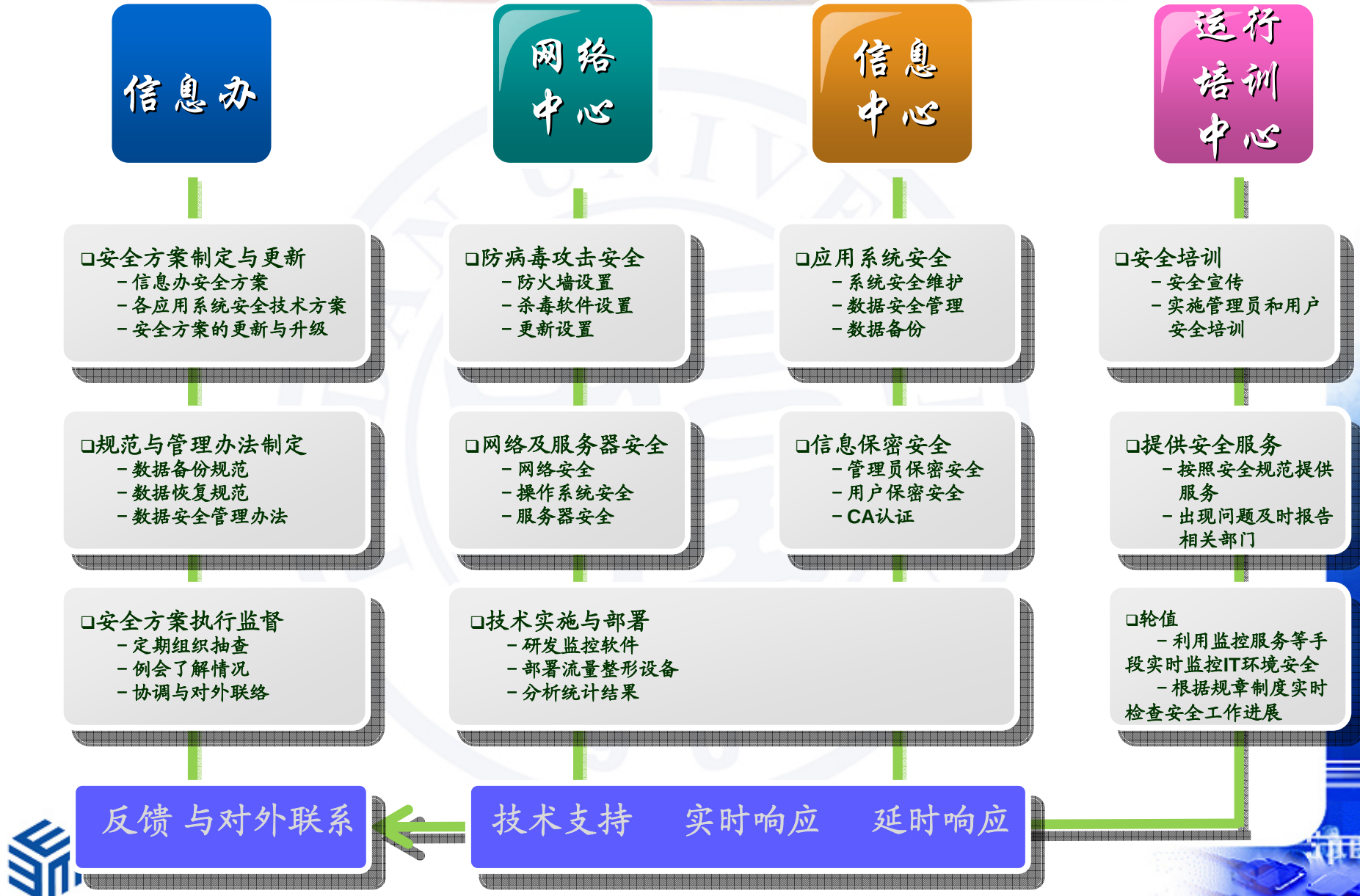
信息中心

- ❑应用系统安全
  - 系统安全维护
  - 数据安全管理
  - 数据备份
- ❑信息保密安全
  - 管理员保密安全
  - 用户保密安全

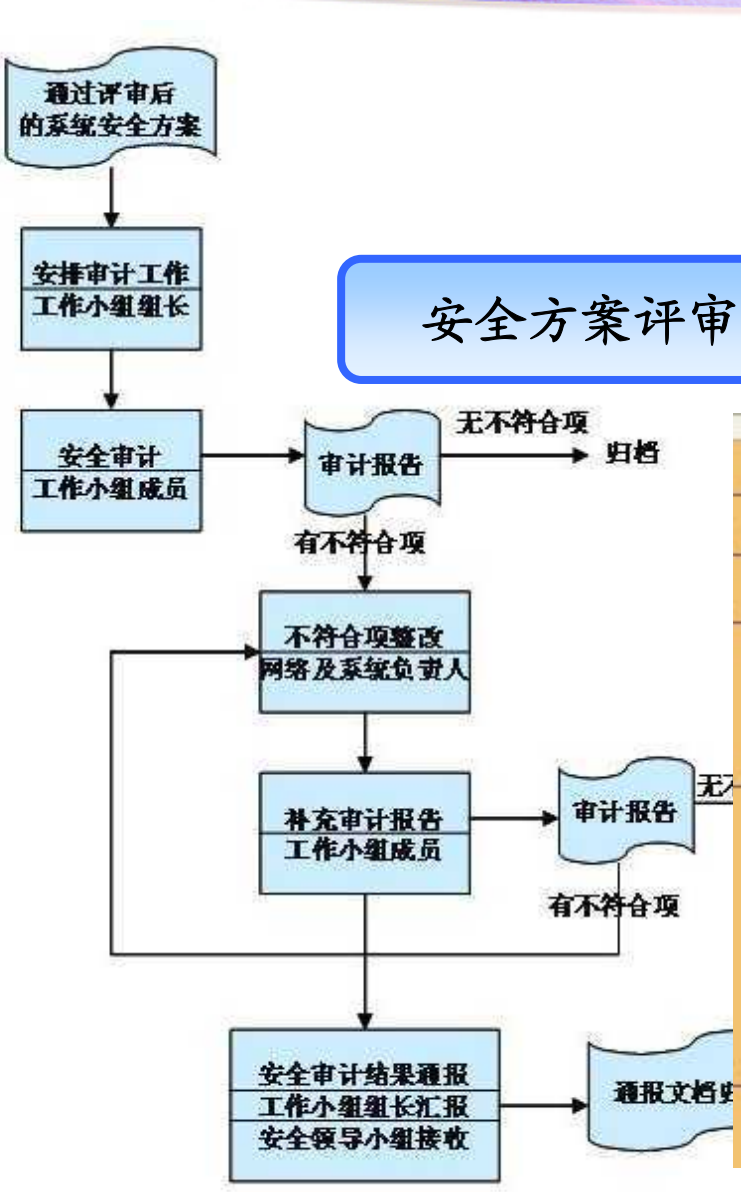
运行培训中心

- ❑保障网络及系统提供安全服务
  - 按照安全规范提供服务
  - 出现安全问题及时报告相关部门
- ❑安全培训
  - 安全宣传
  - 实施管理员和用户安全培训

应急响应机制


信息办
网络中心
信息中心
运行培训中心
❑安全方案制定与更新
– 信息办安全方案
– 各应用系统安全技术方案
– 安全方案的更新与升级
❑防病毒攻击安全
– 防火墙设置
– 杀毒软件设置
– 更新设置
❑应用系统安全
– 系统安全维护
– 数据安全管理
– 数据备份
❑安全培训
– 安全宣传
– 实施管理员和用户安全培训
❑规范与管理办法制定
– 数据备份规范
– 数据恢复规范
– 数据安全管理办法
❑网络及服务器安全
– 网络安全
– 操作系统安全
– 服务器安全
❑信息保密安全
– 管理员保密安全
– 用户保密安全
– CA认证
❑提供安全服务
– 按照安全规范提供服务
– 出现问题及时报告相关部门
❑安全方案执行监督
– 定期组织抽查
– 例会了解情况
– 协调与对外联络
❑技术实施与部署
– 研发监控软件
– 部署流量整形设备
– 分析统计结果
❑轮值
– 利用监控服务等手段实时监控IT环境安全
– 根据规章制度实时检查安全工作进展
反馈 与对外联系
技术支持
实时响应
延时响应

健全保障体系



制度保障

安全方案评审

安全审计制度

安全工作小组审计安排表

完成日期	审计人	被审计方案名称	是否提交审计报告	结果	问题跟踪	解决负责人
2005-1-11	孙毅	磁带机备份方案（V1.1）	应提交	因孙毅太忙，审计报告未提交	跟踪完成	孙毅
2005-1-11	刘洋	复旦大学OA系统安全运行管理方案（V1.2）	应提交	符合点：双机热备存在。 有条件符合点：数据备份及故障恢复策略已变更，与方案不符。已与项目沟通并完成安全方案的修订，欣银前发出。 不符合点：服务器日志无备份。（服务器迁移）	方案修订并完成评审	王明洁
2005-1-11	向望	URP系统安全运行管理方案（V1.0）	应提交	符合点：DB2单机备份；IDS数据备份；Solaris系统基本安全；Solaris日志审查；DB2配置及更新；报表模板异地备份；报表服务器杀毒软件安装与更新；IBM HTTP Server永久备份。 不符合点：WebSphere App. Server双机备份（业务系统部份）因服务器迁移导致磁盘空间不够；报表服务器安全基本保证，还需优化（一直服务中，不敢改动）。	确定磁盘空间不够原因并制定出解决方案，修补缺陷。在URP业务不够繁忙时优化报表服务器安全。	张凯 王彬
2005-1-11	吴庆杰	虚拟校园安全运行管理方案（V1.2）	应提交	符合点：Web服务器；数据库服务器；课件资源； 不符合点：NAS服务器磁带备份	无法弥补，在此	

健全保障体系

安 全 审 计 报 告

审计人员	陈旭光	报告日期	2005-9-14
被审计方名称	磁带机备份		
检 查 日 期	2005-9-14	审计依据	磁带机备份方案（V1.2）

审 计 结 果

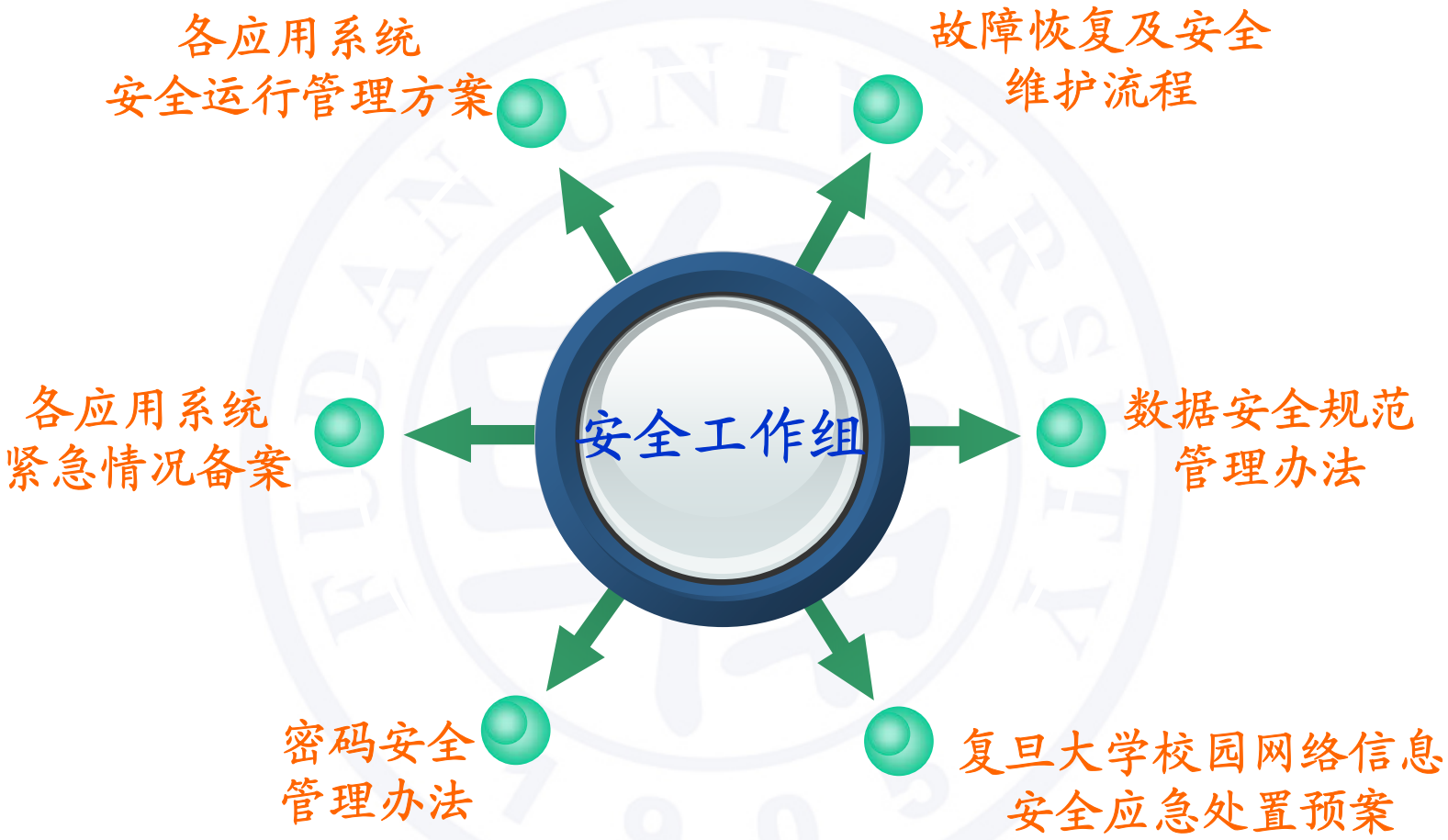
符合点	虚拟校园 db2 数据库联机备份文件	
	虚拟校园 db2 数据库联机 log 文件	
	虚拟校园备份期限	
	虚拟校园 CPQNAS 备份 统一身份认证 IDS 备份 URP 系统数据库每日备份	
	URP 系统数据库每周备份	
	URP 系统 websphere 备份	
有条件的符合点	数据库每日备份时间（1 点）	条件:
	磁带机每日备份时间（2：30 点）	条件:
	WebSphere App. Server 备份（业务系统部分）	条件:
	WebSphere App. Server 备份（平台部分）	条件:
	虚拟校园 db2 数据库恢复测试	原因:
	虚拟校园 CPQNAS 恢复测试	原因:

工作报告单

时间：2005年9 月12 日

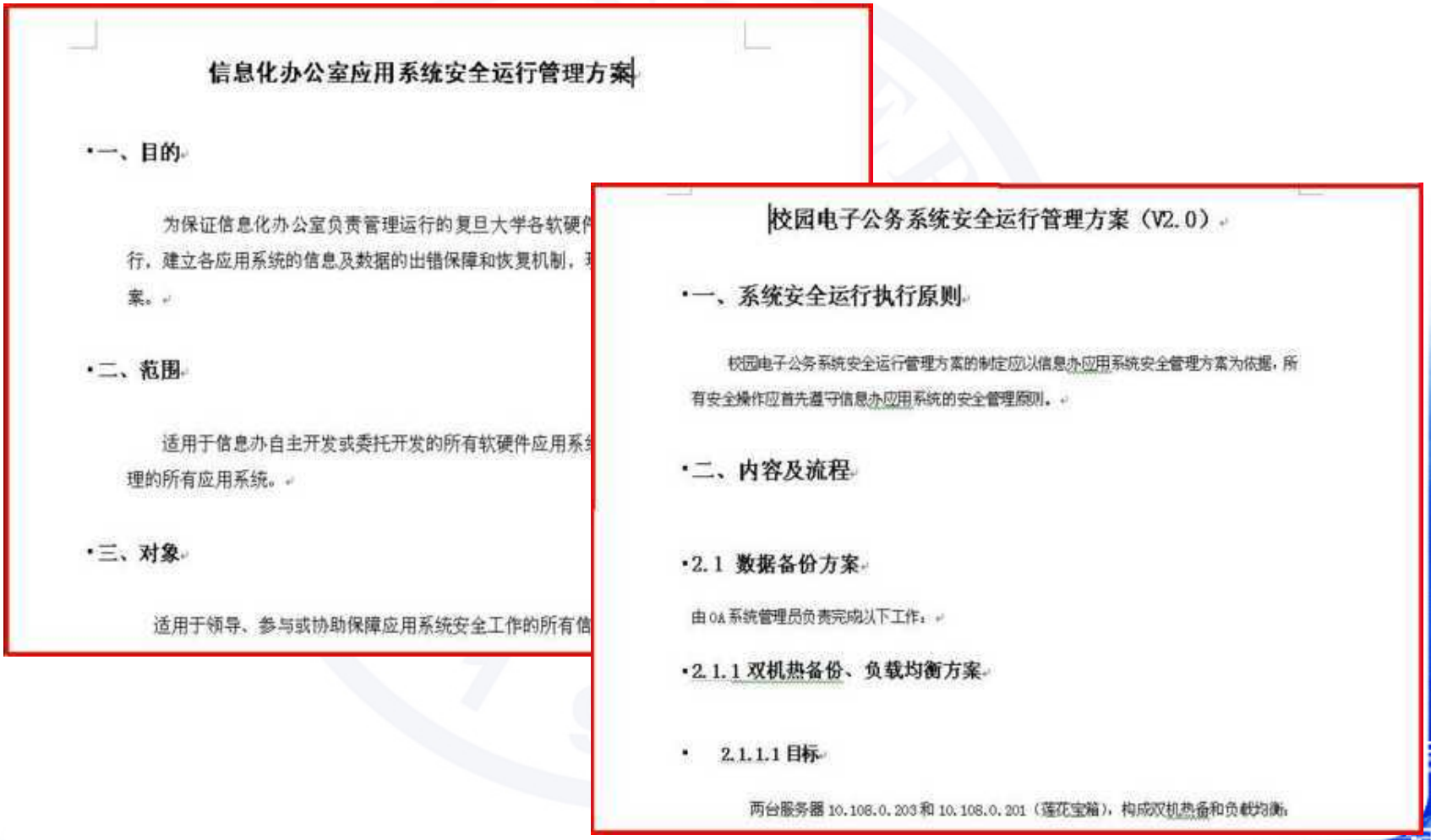
成员姓名	所在项目/分类	计划完成工作	计划完成日期段	计划所用时间(h)	潜在风险	完成工作	完成日期段
[illegible]	1教务系统	[illegible]	9月12日-9月16日	12		[illegible]	9月12日-9月1[illegible]
	2教务系统	[illegible]	9月12日-9月16日	8		[illegible]	9月12日-9月1[illegible]
	3资产系统	[illegible]	9月12日-9月13日	8		[illegible]	9月13日-9月1[illegible]
	4资产系统	[illegible]	9月12日-9月16日	8		[illegible]	9月14日
	5工作计划	制定工作计划	9月12日	2		制定工作计划	9月12日
						[illegible]	9月15日-9月1[illegible]
[illegible]	[illegible]	[illegible]	9月12日-9月15日	32		[illegible]	9月12日-9月[illegible]
	学工系统	[illegible]	9月16日	4		[illegible]	
						[illegible]	9月15日
						[illegible]	9月15日
	共享数据库	工作计划和总结	9月12日-9月12日	2		[illegible]	
	共享数据库	[illegible]	9月12日-9月12日	6		[illegible]	

规范管理制度


各应用系统
安全运行管理方案
故障恢复及安全
维护流程
各应用系统
紧急情况备案
安全工作组
数据安全规范
管理办法
密码安全
管理办法
复旦大学校园网络信息
安全应急处置预案

规范管理制度

信息办制定安全运行管理方案



信息化办公室应用系统安全运行管理方案

一、目的

为保证信息化办公室负责管理运行的复旦大学各软硬件
行，建立各应用系统的信息及数据的出错保障和恢复机制，
案。

二、范围

适用于信息办自主开发或委托开发的所有软硬件应用系
理的所有应用系统。

三、对象

适用于领导、参与或协助保障应用系统安全工作的所有信

校园电子公务系统安全运行管理方案（V2.0）

一、系统安全运行执行原则

校园电子公务系统安全运行管理方案的制定应以信息办应用系统安全管理方案为依据，所有安全操作应首先遵守信息办应用系统的安全管理原则。

二、内容及流程

2.1 数据备份方案

由OA系统管理员负责完成以下工作：

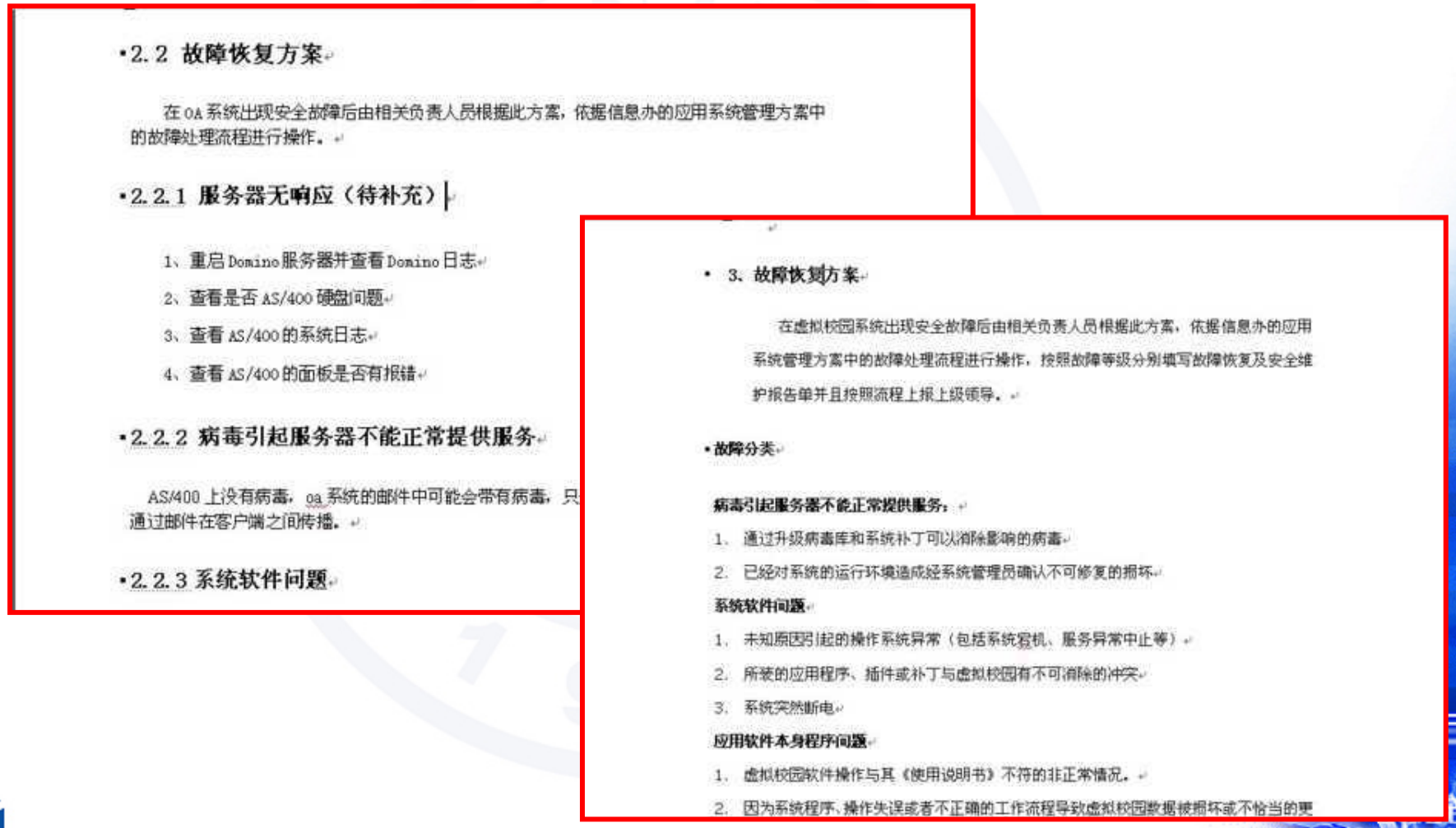
2.1.1 双机热备份、负载均衡方案

2.1.1.1 目标

两台服务器10.108.0.203和10.108.0.201（莲花宝箱），构成双机热备和负载均衡。

规范管理制度

信息办制定故障恢复方案



·2.2 故障恢复方案

在OA系统出现安全故障后由相关负责人员根据此方案，依据信息办的应用系统管理方案中的故障处理流程进行操作。

·2.2.1 服务器无响应（待补充）

1、重启Domino服务器并查看Domino日志

2、查看是否AS/400硬盘问题

3、查看AS/400的系统日志

4、查看AS/400的面板是否有报错

·2.2.2 病毒引起服务器不能正常提供服务

AS/400上没有病毒，oa系统的邮件中可能会带有病毒，只通过邮件在客户端之间传播。

·2.2.3 系统软件问题

· 3、故障恢复方案

在虚拟校园系统出现安全故障后由相关负责人员根据此方案，依据信息办的应用系统管理方案中的故障处理流程进行操作，按照故障等级分别填写故障恢复及安全维护报告单并且按照流程上报上级领导。

·故障分类

病毒引起服务器不能正常提供服务：

1. 通过升级病毒库和系统补丁可以消除影响的病毒
2. 已经对系统的运行环境造成经系统管理员确认不可修复的损坏

系统软件问题

1. 未知原因引起的操作系统异常（包括系统宕机、服务异常中止等）
2. 所装的应用程序、插件或补丁与虚拟校园有不可消除的冲突
3. 系统突然断电

应用软件本身程序问题

1. 虚拟校园软件操作与其《使用说明书》不符的非正常情况。
2. 因为系统程序、操作失误或者不正确的工作流程导致虚拟校园数据被损坏或不恰当的更

规范管理制度

信息办通过制定《应用系统数据备份方案》模板，生成具体应用系统的数据备份方案

应用系统数据备份方案（模板）

应用系统名称	人事系统	
域名	http://www.urp.fudan.edu.cn	
系统服务器 IP	多台机器 见下表	
系统管理员	韩立媛 吴庆杰	
数据备份策略		
服务器是否存在	Y	
服务器名称及 IP	URP Httpserver 61.129.42.65	
服务器登陆方式	Ssh	
数据备份操作员	韩立媛	
本地备份策略	备份文件源及说明	/usr/local/apache2/目录
	备份目的地及说明	/backup/apache.tar.gz
	目的文件保留周期	永久
	是否自动执行	否
	备份时间点	初始化一次
	备份周期	无
异	备份文件源及说明	/backup/apache.tar.gz

规范管理制度

信息办制定数据安全规范管理办法

信息办数据安全规范管理办法

为保证信息办开发的各应用系统的顺利运行，在系统进行测试阶段以后，即需要进行各种信息及数据的导入工作。复旦大学相关职能部门为配合系统按期交付并运行，将系统数据交予信息办，信息办负责保证接收到数据的安全使用。

信息化办公室为保证数据的安全，特制定了严格的管理规范和流程。对数据的流向及涉及人员都严格控制，能够保证数据的安全使用。

一、 所有原始（真实）数据均由信息化办公室主任直接保管；

二、 对数据安全等级进行划分，分为完全保密数据，保密数据，非保密数据。对不同保密等级的数据纳入不同的管理流程进行分级管理；

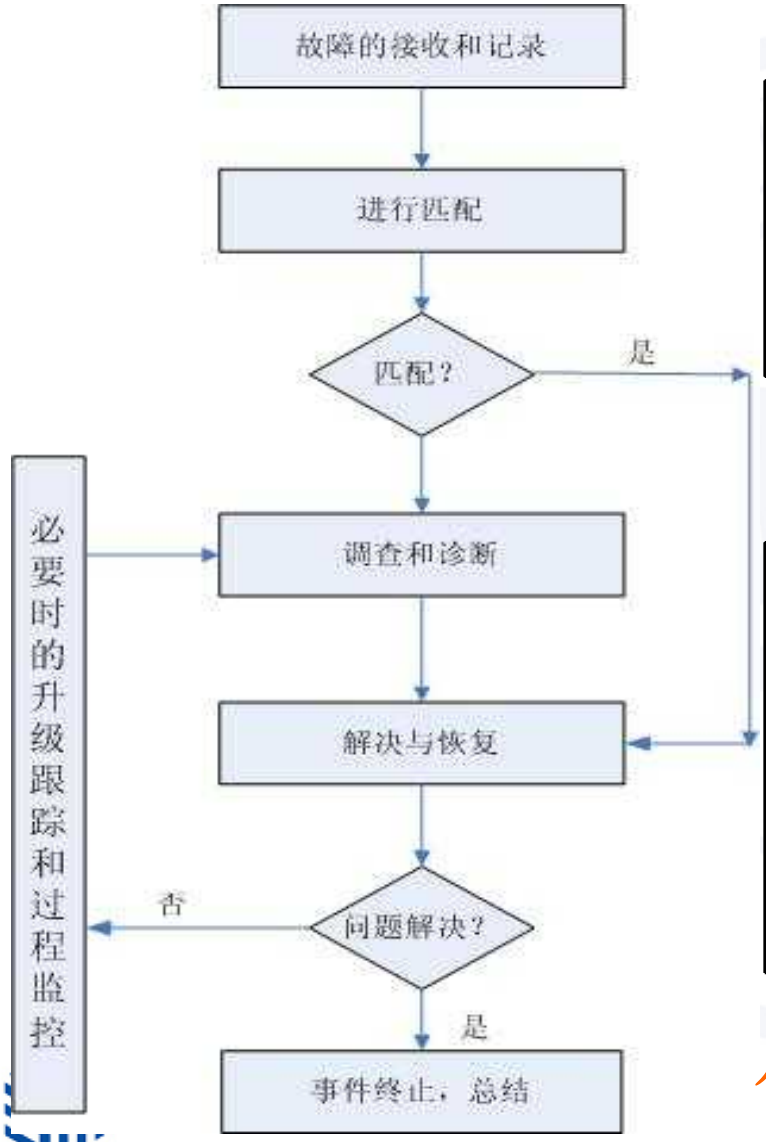
三、 在系统进行测试阶段需要数据导入时，数据使用者或项目组（含开发方）应提交书面的数据使用申请，申请中应明确说明使用数据的目的和导入数据范围，申请上应有项目负责人的签名。对于不影响测试的数据应选择在试运行后期导入。

下表为不同安全等级数据的导入流程：

数据安全	数据	数据安全	是否签	数据导入流程

E-campus

故障处理流程



故障级别与处理时间要求

故障级别	响应时间	确定初步方案时间	采取措施的时间
A级故障	10分钟	<0.5小时	1小时内采取措施
B级故障	30分钟之内	4小时	8小时之内采取措施
C级故障	1小时之内	24小时	

故障的级别及上报时间

上报时间	A级故障	B级故障	C级故障
接到报告	主管、室主任	主管	组长
10分钟	中心主任		
30分钟		室主任	
4小时		中心主任	主管
1个工作日			室主任

信息办制定故障处理流程

故障处理流程

等级		故障定义					
		1	2	3	4	5	6
0	影响全网	全网瘫痪					
1	影响多个汇聚点	核心设备端口损坏	核心设备掉电或损坏	核心路由配置损坏	防火墙配置过强	防火墙死机或损坏	核心设备死机
		计费网关死机	负载均衡器掉电或损坏	带宽管理器掉电或损坏	网络病毒流量过大		
2	影响单个会聚点	接入设备配置丢失	汇聚点路由配置丢失	汇聚点端口损坏	汇聚层机器瘫痪	接入设备机器瘫痪	
3	应用故障	服务器硬件故障	服务器掉电	应用停止服务	数据备份停止		
4	影响单台或多台计算机	交换机端口损坏	光块损坏	光收损坏	光纤跳线损坏	交换机掉电	汇聚点掉电
		光纤收发器掉电					
5	单机网络故障	网线损坏	模块损坏	跳线损坏	配线架损坏	跳线未插	
6	单机系统故障	操作系统原因	操作失误	网络设置错误	硬件损坏	软件故障	

信息办制定IT运行故障定义及处置方案，将运行故障分为7个等级，以助于规范处理流程设计

故障处理流程

等级	故障状况	故障说明	人员调度	处置机制
零	全网瘫痪	全校网络完全停止运行，无法查明原因	运行中心、网络中心、专家组	向校领导和校办、党办汇报,通知各单位网管员，。第一时间组织（外聘专家组和）内部技术力量研究解决。如发现人为因素造成，尽可能隔离和屏蔽，先恢复网络正常运转，再通知整改。
	全网瘫痪	全校网络完全停止运行，能查明原因	运行中心、网络中心、	
一	核心设备端口损坏	端口包括以太网口，光块端口等	运行、网络中心、	通知受影响的单位网管员，并向部门主任汇报； 因修改配置引起的，应第一时间还原回原配置，保证网络正常运行后择期修改配置后重新部署； 因设备故障引起的，尽快通知设备产商更换或维修，第一时间使用备件替换； 设备掉电引起的，须追查掉电原因，发掘潜在隐患； 如发现人为因素造成，尽可能隔离和屏蔽，先恢复网络正常运转，再通知整改。
	核心设备掉电		运行中心	
	核心路由配置损坏	路由表的丢失，端口的查封等	网络中心	
	防火墙配置过强	端口的开放，策略的应用	网络中心	
	防火墙死机	负载过大，或其他无法运行	网络中心	
	核心设备死机		运行中心	
	计费网关死机	负载过大，或其他原因死机	网络中心	
	负载均衡器掉电或损坏	单点故障导致出口断线	运行中心	
	带宽管理器掉电或损坏	单点故障导致出口断线	网络中心	
	网络病毒流量过大	病毒造成大量流量阻塞网络出口	网络中心	
二	接入设备配置丢失	路由表的丢失，端口的查封等	网络中心	
	汇聚点路由配置丢失	路由表的丢失，端口的查封等	网络中心	
	汇聚点端口损坏	端口包括以太网口，光块端口等	网络中心	
	汇聚层机器瘫痪	负载过大，或其他无法运行	网络中心	
	接入设备机器瘫痪	负载过大，或其他无法运行	运行中心	

故障处理流程定义

E-campus

完备的应急响应流程

监控服务器

Monitor

短信发送器

7*24值班响应

短信报警

问题解决，
记录在案

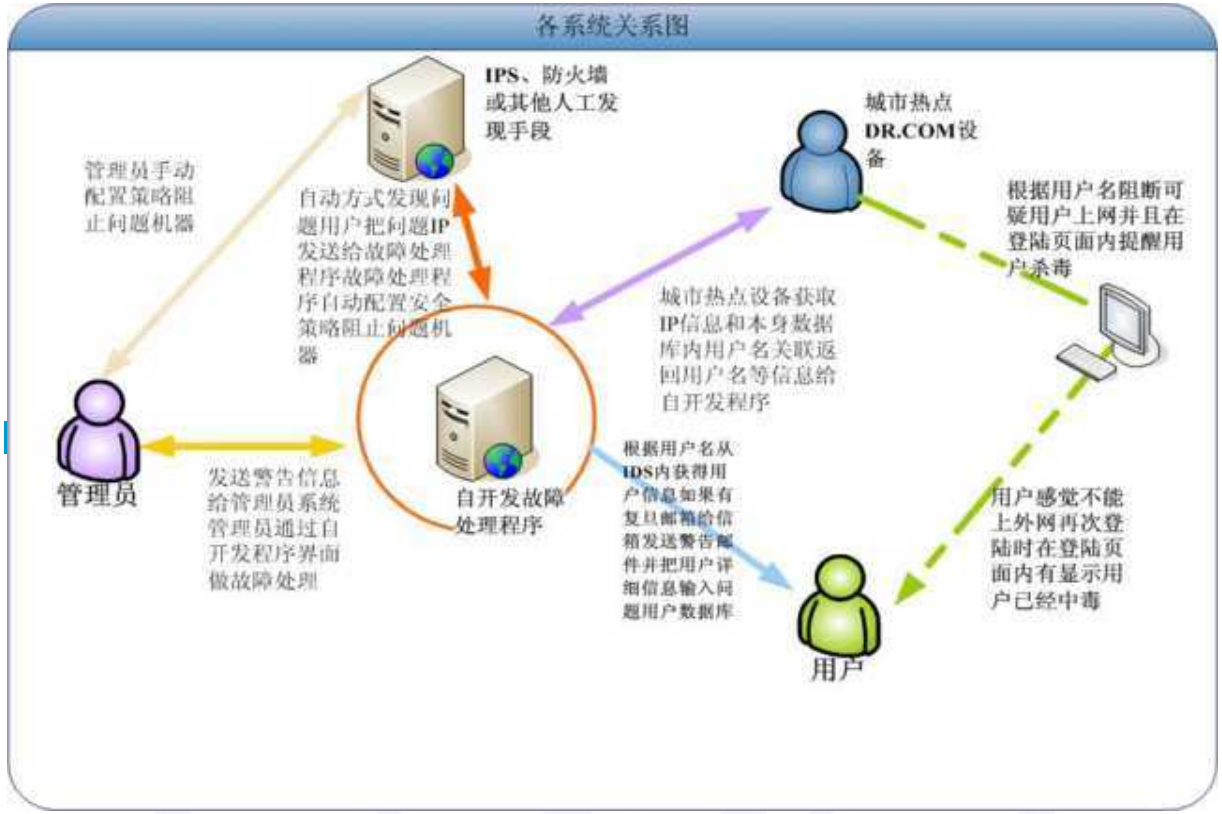
特殊情况，
及时上报

管理人员处理

校园网/系统/主要应用

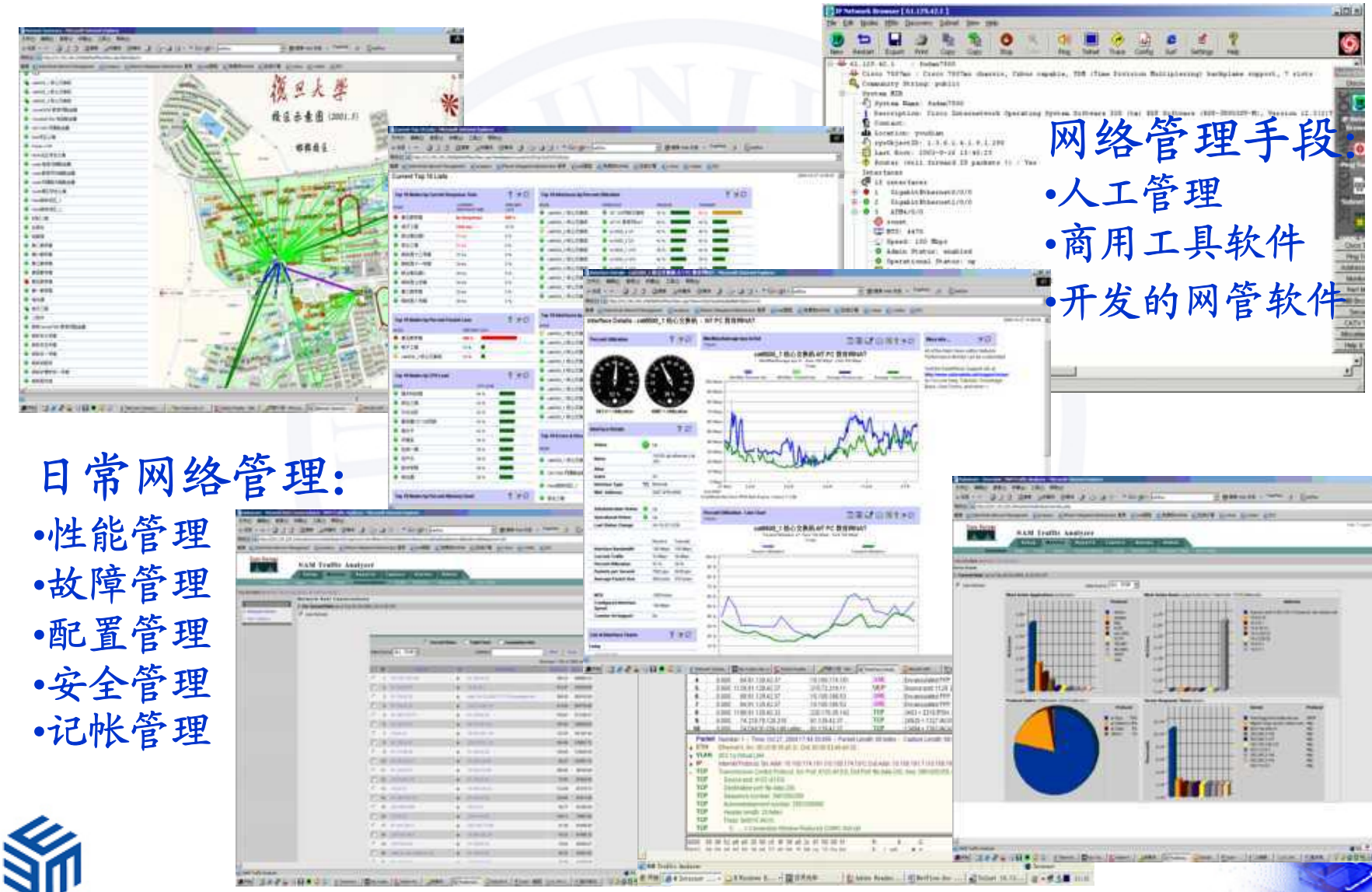
运行中心的应急响应流程

整合和规划网络安全防范技术流程



复旦大学的网络安全不应该是一个个单独的系统，应该是一个互相关联的网络安全系统。各种网络安全硬件，软件，管理人员等在统一程序的调度下成为这个系统的一个组成部分。最终的目的是达到网络问题自动发现和自我防御以及修复

依托技术优势

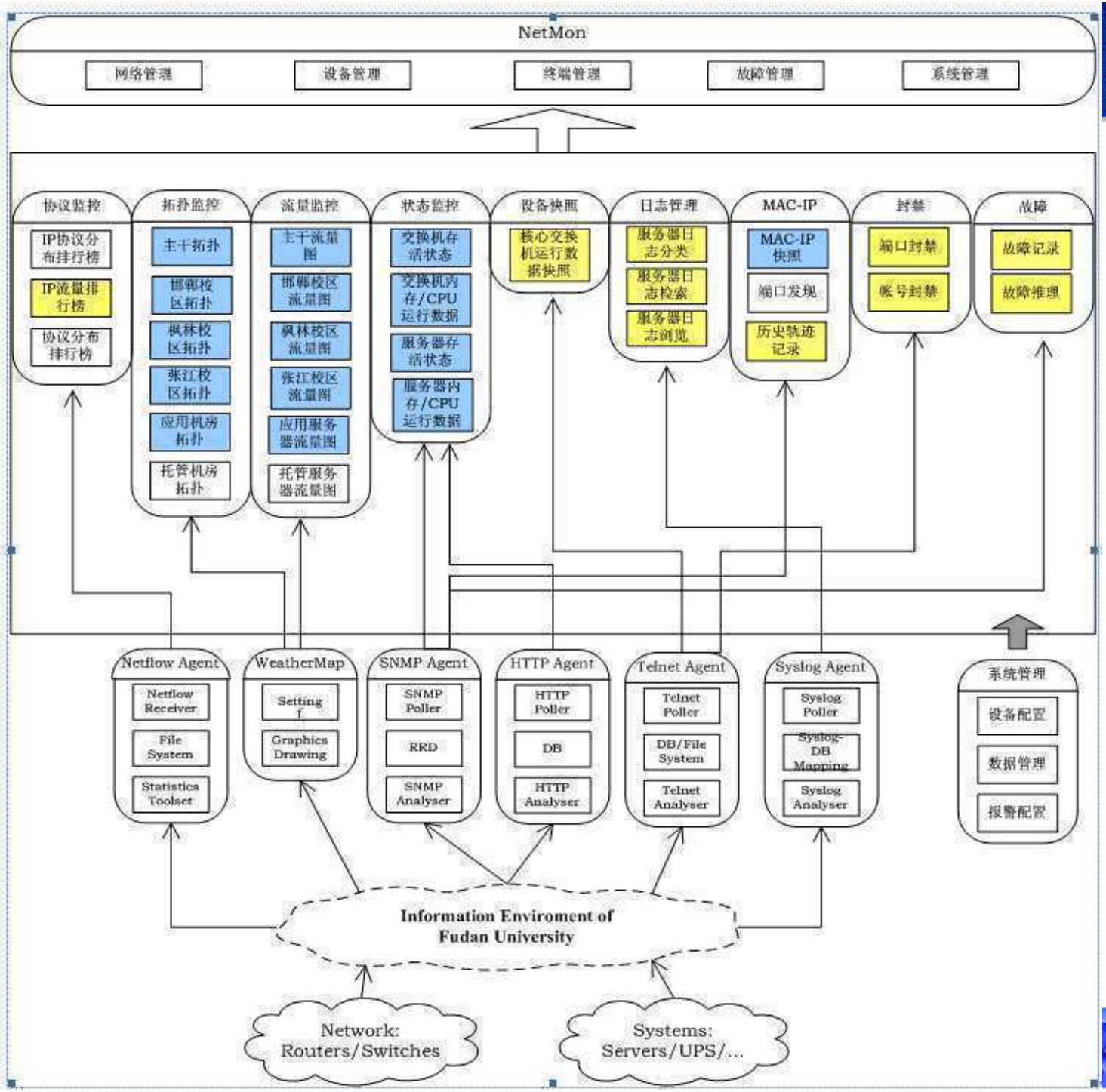


网络管理手段：

- 人工管理
- 商用工具软件
- 开发的网管软件

日常网络管理：

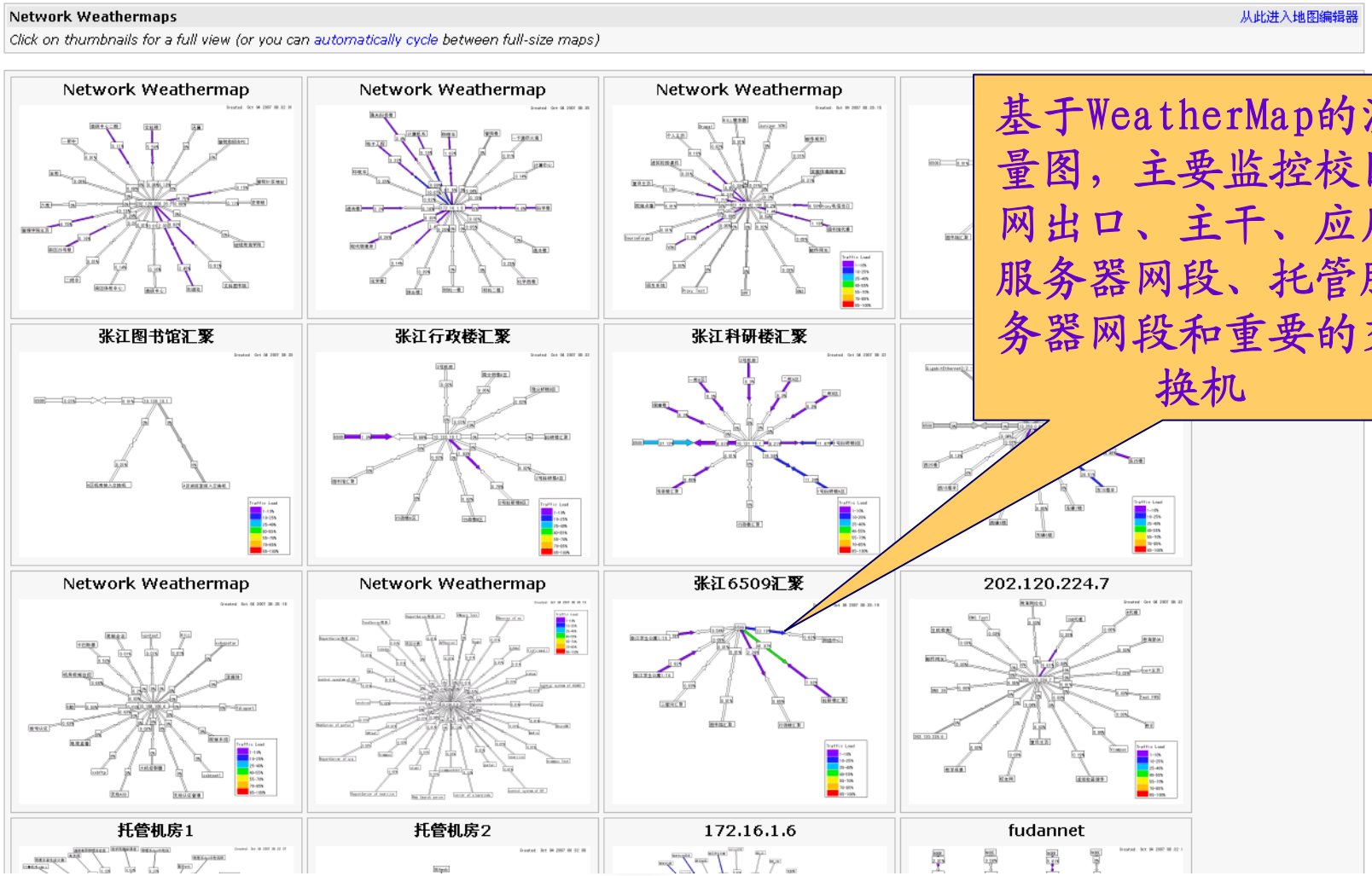
- 性能管理
- 故障管理
- 配置管理
- 安全管理
- 记帐管理

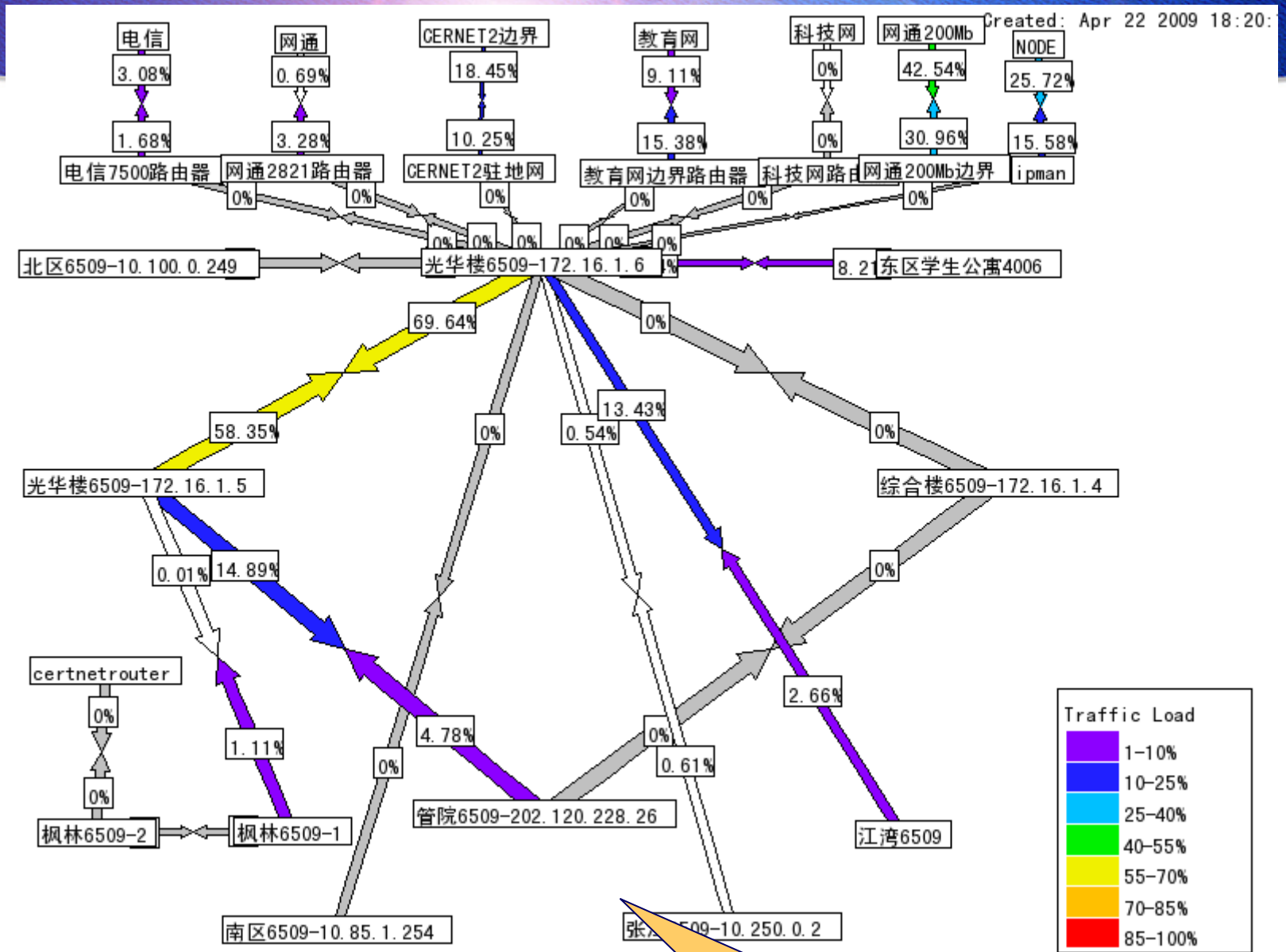

NetMon
网络管理
设备管理
终端管理
故障管理
系统管理
协议监控
IP协议分布排行榜
IP流量排行榜
协议分布排行榜
拓扑监控
主干拓扑
邯郸校区拓扑
枫林校区拓扑
张江校区拓扑
应用机房拓扑
托管机房拓扑
流量监控
主干流量图
邯郸校区流量图
枫林校区流量图
张江校区流量图
应用服务器流量图
托管服务器流量图
状态监控
交换机存活状态
交换机内存/CPU运行数据
服务器存活状态
服务器内存/CPU运行数据
设备快照
核心交换机运行数据快照
日志管理
服务器日志分类
服务器日志检索
服务器日志浏览
MAC-IP
MAC-IP快照
端口发现
历史轨迹记录
封禁
端口封禁
帐号封禁
故障
故障记录
故障推理
Netflow Agent
Netflow Receiver
File System
Statistics Toolset
WeatherMap
Setting f
Graphics Drawing
SNMP Agent
SNMP Poller
RRD
SNMP Analyser
HTTP Agent
HTTP Poller
DB
HTTP Analyser
Telnet Agent
Telnet Poller
DB/File System
Telnet Analyser
Syslog Agent
Syslog Poller
Syslog-DB Mapping
Syslog Analyser
系统管理
设备配置
数据管理
报警配置
Information Enviroment of Fudan University
Network: Routers/Switches
Systems: Servers/UPS/...

依托技术优势

功能	描述
流量图	通过SNMP获取网络设备端口流量并以RRD图显示
阈值面板	设定各端口流量阈值并显示当前状态
状态面板	网络设备存活判断
子网探测	子网地址探测，用于实地址子网
日志	交换机/路由器/服务器的syslog日志收集与显示
MAC	IP-MAC(计数)、Vlan、端口的实时采集与对应关系表
拓扑图	网络拓扑管理，辅助运行服务
服务器	服务器实时运行状态监控：CPU|MEM|服务|进程|磁盘|端口|连通性|基本网络协议
实地址	基于Flow-tools的Netflow采集、存储和计算；提供实地址网络流量等相关功能的监视
配置管理	交换机配置备份以及变更提示

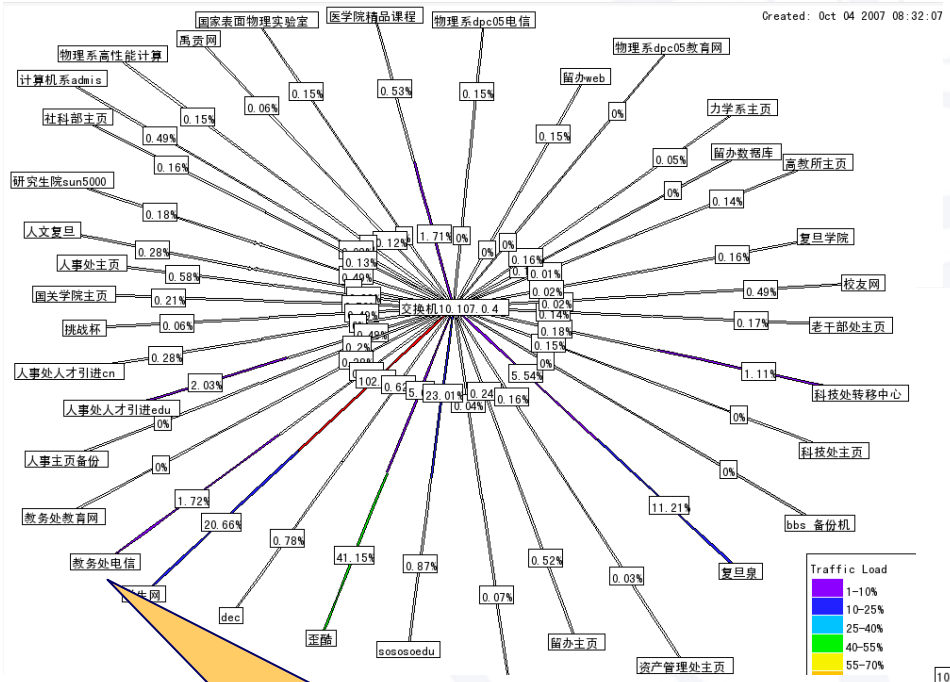
依托技术优势


Network Weathermaps
从此进入地图编辑器
Click on thumbnails for a full view (or you can automatically cycle between full-size maps)
Network Weathermap
Network Weathermap
Network Weathermap
张江图书馆汇聚
张江行政楼汇聚
张江科研楼汇聚
Network Weathermap
Network Weathermap
张江6509汇聚
202.120.224.7
托管机房1
托管机房2
172.16.1.6
fudannet
基于WeatherMap的流量图，主要监控校园网出口、主干、应用服务器网段、托管服务器网段和重要的交换机


Created: Apr 22 2009 18:20:
电信
3.08%
1.68%
电信7500路由器
网通
0.69%
3.28%
网通2821路由器
CERNET2边界
18.45%
10.25%
CERNET2驻地网
教育网
9.11%
15.38%
教育网边界路由器
科技网
0%
0%
科技网路由
网通200Mb
42.54%
30.96%
网通200Mb边界
NODE
25.72%
15.58%
ipman
北区6509-10.100.0.249
光华楼6509-172.16.1.6
8.21东区学生公寓4006
69.64%
58.35%
光华楼6509-172.16.1.5
0%
13.43%
0.54%
综合楼6509-172.16.1.4
0.01%
14.89%
certnetrouter
1.11%
枫林6509-2
枫林6509-1
4.78%
管院6509-202.120.228.26
0.61%
2.66%
江湾6509
南区6509-10.85.1.254
张[illegible]509-10.250.0.2
Traffic Load
1-10%
10-25%
25-40%
40-55%
55-70%
70-85%
85-100%

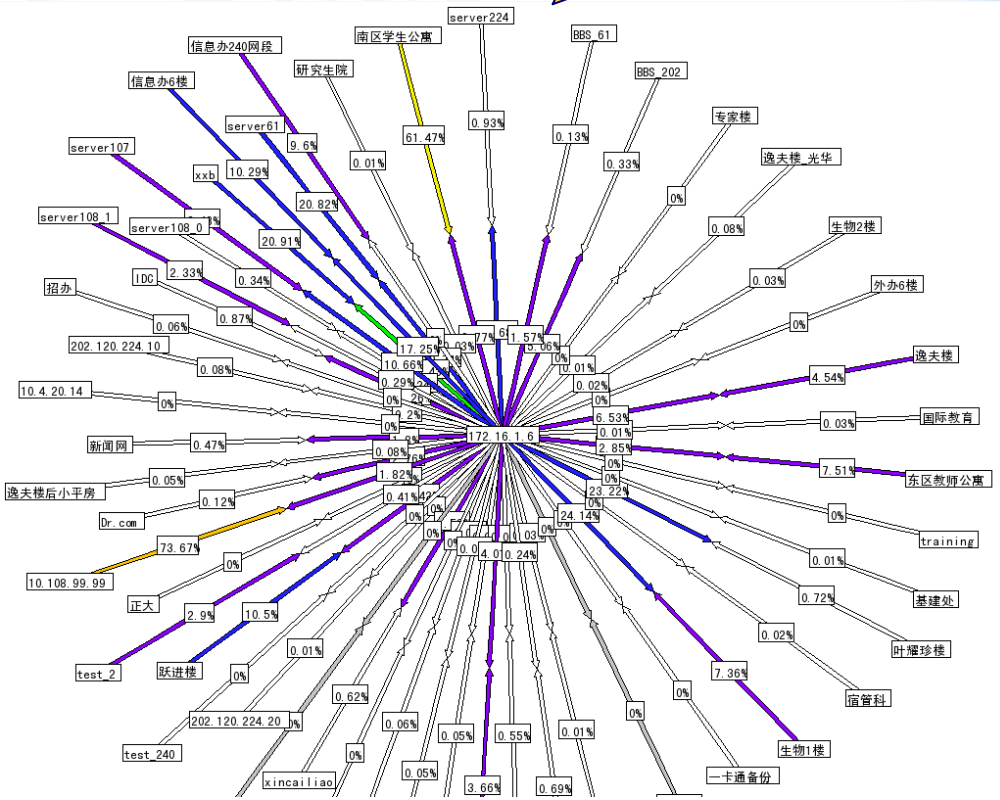
校园主干流量分布图

依托技术优势

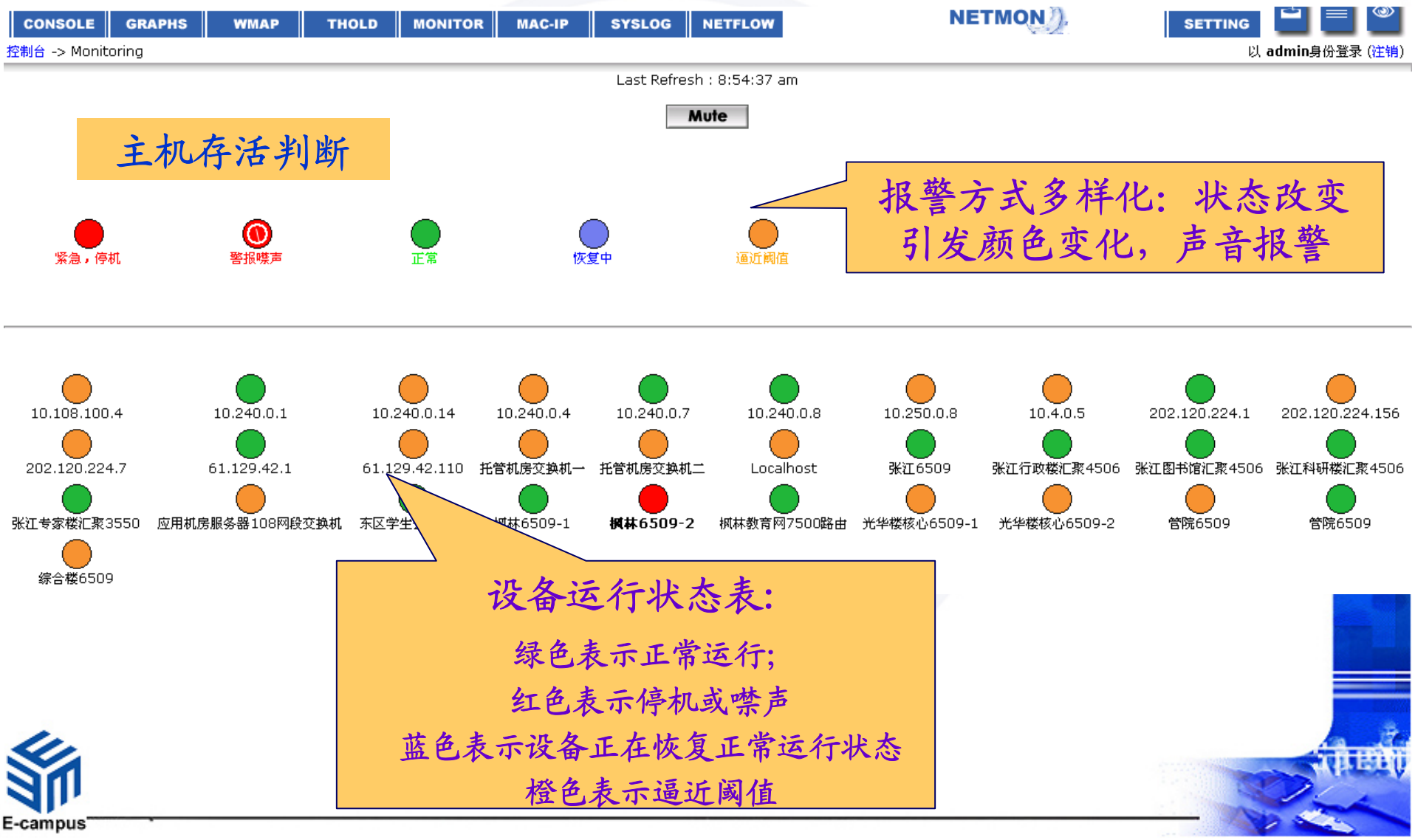


托管服务器网段流量分布图

主干交换机之一的端口流量分布图

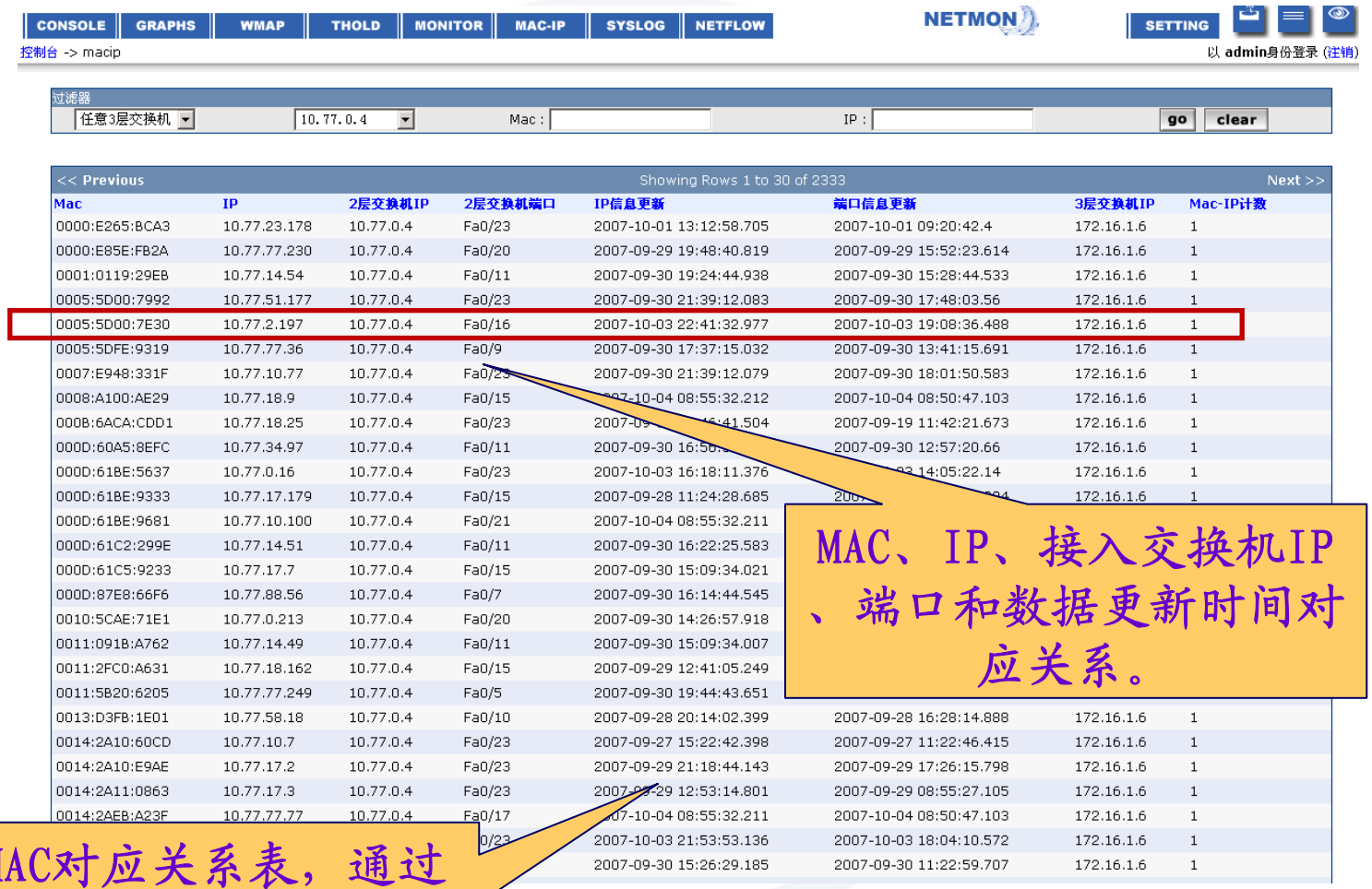


依托技术优势



E-campus

依托技术优势

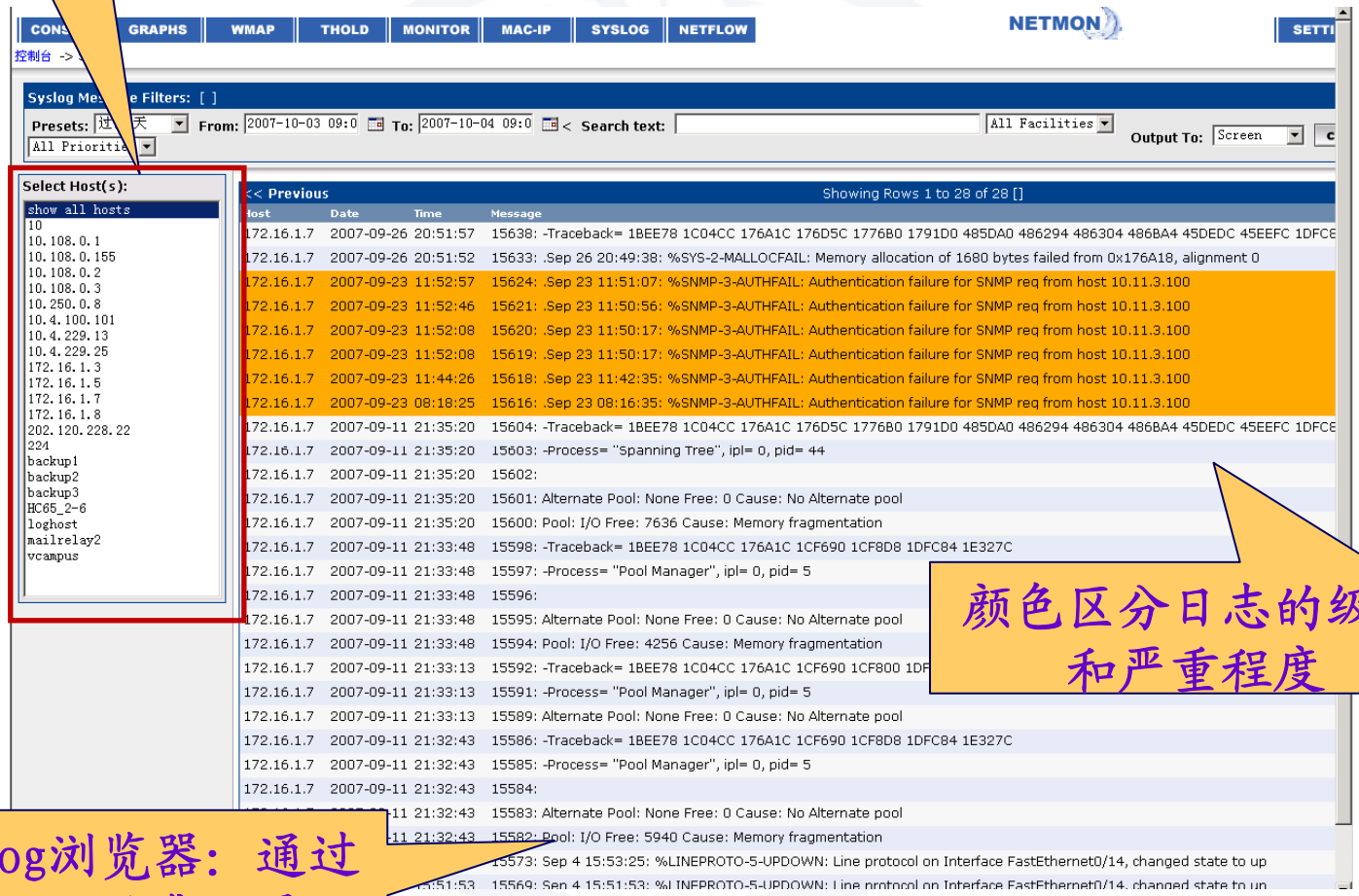


MAC、IP、接入交换机IP、端口和数据更新时间对应关系。

IP-MAC对应关系表，通过SNMP从2层、3层交换机定时轮询，查找异常信息

依托技术优势

设备列表



颜色区分日志的级别和严重程度

Syslog浏览器：通过SyslogNG收集和展示设备标准化日志

依托技术优势

IP流量监视表

61.129.42.33 昨日流量统计

Port	Flows	Octects	Packets
80	434838	3837899716	4154242
9694	110059	823122536	1872452
53	221910	61081340	285087
48836	50	6849645	135760
50645	12	3726804	71669
48837	43	3696744	67826
50640	7	3644800	70092
48361	23	2956737	58544
443	527	2859907	23556
49677	22	2173980	41807
48355	9	1605493	29287
48804	12	1328766	26200
49190	2	1281783	24246
48784	17	1121393	20624
48783	10	1116772	20530
48746	11	844011	15311
48747	6	831466	15107
48803	8	730166	13123
42616	76	594810	11167
32904	124	547853	10244

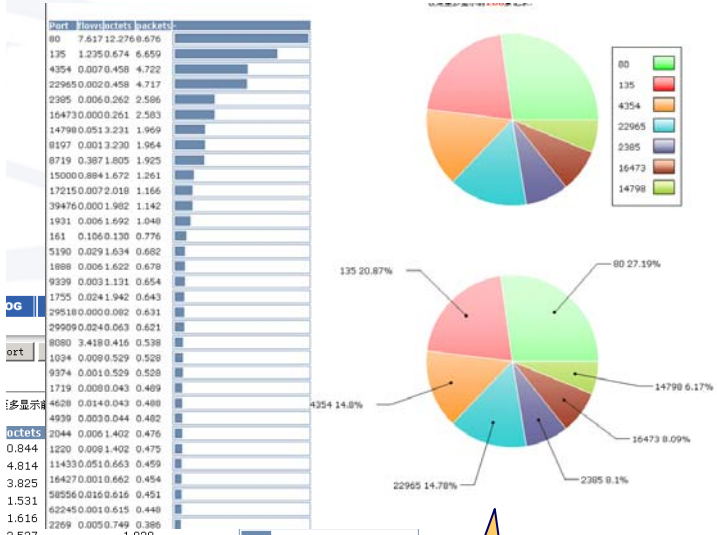
61.129.42.33 昨日流量统计

Src IPAddr	Dst IPAddr	Flows	Octects	Packets
61.129.42.33	220.181.38.206	133446	1870773054	1672370
61.129.42.33	10.83.29.160	118383	137885170	2577887
61.129.42.33	220.181.19.171	8365	112040418	103725
61.129.42.33	220.181.19.159	8475	107055128	98975
61.129.42.33	60.191.80.86	4454	49419116	46319
61.129.42.33	219.136.247.113	2070	34649363	29884
61.129.42.33	220.181.19.166	2952	29490044	28218
61.129.42.33	60.191.80.75	2504	29056667	27077
61.129.42.33	61.135.166.234	44855	26717894	210970
61.129.42.33	60.191.80.81	2389	24816322	23943
61.129.42.33	208.68.136.5	2237	24551379	23015
61.129.42.33	66.249.67.187	1488	24248985	21388
61.129.42.33	60.191.80.78	1940	20218768	19023
61.129.42.33	218.93.16.74	1476	19778731	17739
61.129.42.33	60.191.80.77	1954	19701037	18911
61.129.42.33	219.136.247.70	1054	17721407	15332
61.129.42.33	192.168.185.68	717	17667834	36707
61.129.42.33	208.36.144.8	3029	17038944	17059
61.129.42.33	60.191.80.73	1587	16969998	15967
61.129.42.33	60.191.80.79	1771	16710204	16401

61.129.42.5 昨日流量统计

Port	Flows	Octects	Packets
80	355201	9195598720	7868764
25	955	66080	1652

202.120.224.18	202.97.138.85	0.000
202.120.224.18	222.182.37.110	0.000
202.120.224.18	219.218.102.79	0.002
202.120.224.18	222.54.5.24	0.000
202.120.224.18	60.13.159.76	0.000
10.82.0.3	61.152.221.136	0.001
10.240.0.68	222.131.67.220	0.000
202.120.224.18	218.18.101.185	0.000
202.120.224.18	222.37.80.2	0.000
202.120.224.18	58.17.141.7	0.000
202.120.224.18	219.218.83.3	0.029



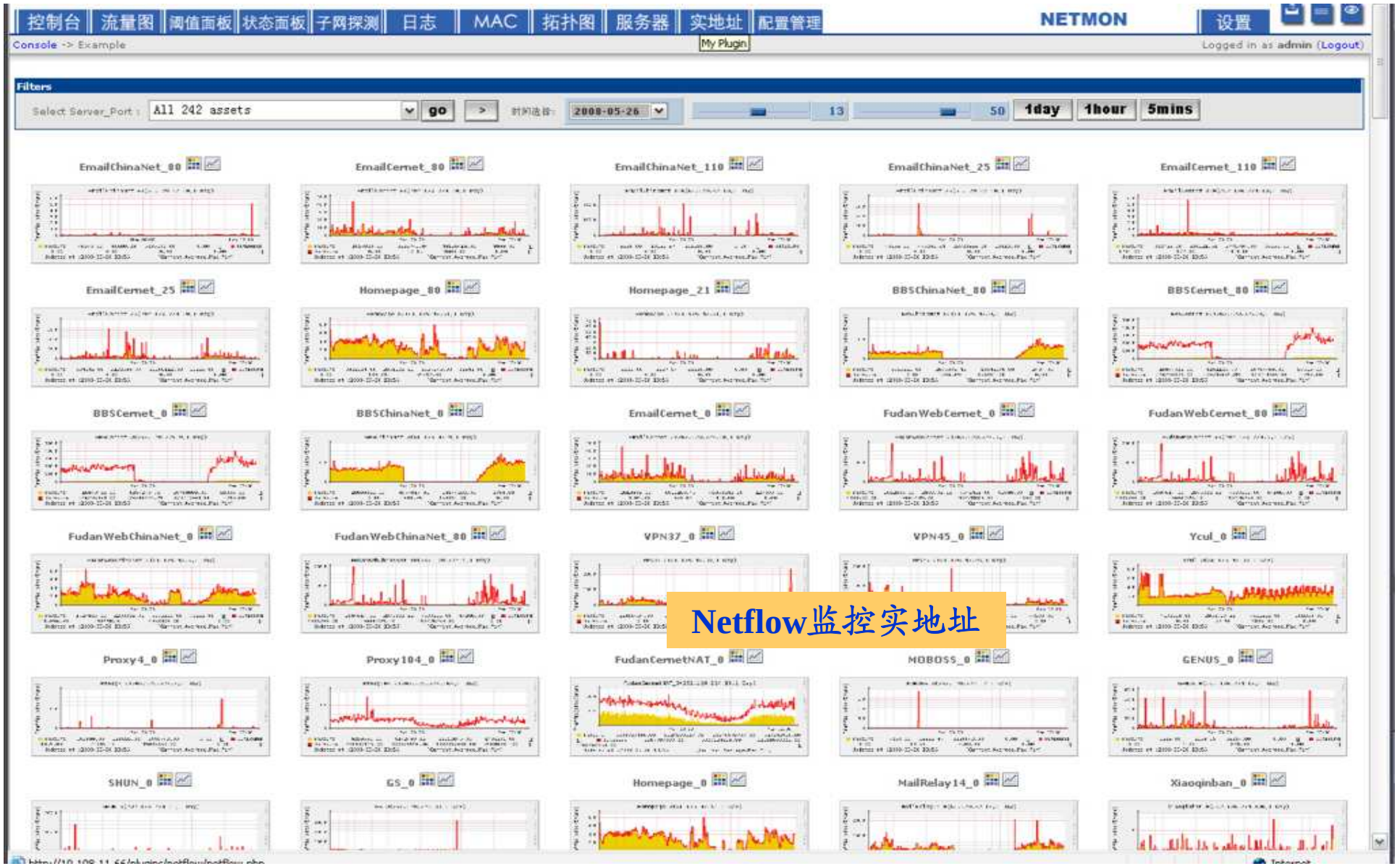
协议分布图

2.527	1.020
0.946	0.937
1.752	0.922
2.055	0.844
1.137	0.796
1.829	0.743
1.843	0.713
0.049	0.671
0.062	0.660
1.508	0.606
1.442	0.593
1.134	0.577
0.050	0.531
1.260	0.531
1.144	0.497
0.066	0.474
0.049	0.457
0.607	0.451
0.034	0.421
0.551	0.393
0.958	0.381
0.029	0.374
0.898	0.374
0.886	0.363
0.485	0.347
0.822	0.346
0.025	0.336

IP流量排行榜

Flow-tools采集Netflow信息，分析协议分布和IP流量

依托技术优势



Netflow监控实地址

依托技术优势

Total Flows	199982970
Total Octets	4331602333193
Total Packets	9175676603
Total Time (1/1000 secs) (flows)	2297582253968
Duration of data (realtime)	86404
Duration of data (1/1000 secs)	4294967292
Average flow time (1/1000 secs)	11488.8895
Average packet size (octets)	472.0744
Average flow size (octets)	21659.8559
Average packets per flow	45.8823
Average flows / second (flow)	46.5622
Average flows / second (real)	2314.5106
Average Kbits / second (flow)	8068.2388
Average Kbits / second (real)	401055.7330

IP packet size distribution:

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480	512	544	576	1024	1536	2048	2560	3072	3584	4096	4608
0.002	0.568	0.170	0.089	0.038	0.021	0.015	0.010	0.008	0.007	0.007	0.004	0.003	0.002	0.002	0.003	0.003	0.002	0.023	0.024	0.000	0.000	0.000	0.000	0.000	0.000

[饼图 百分比] [柱状图 绝对值]

Packets per flow distribution:

1	2	4	8	12	16	20	24	28	32	36	40	44	48	52	60	100	200	300	400	500	600	700	800	900	>900
0.341	0.107	0.165	0.150	0.043	0.020	0.011	0.010	0.015	0.004	0.004	0.004	0.003	0.002	0.004	0.012	0.026	0.069	0.003	0.001	0.001	0.001	0.000	0.000	0.000	0.003

[饼图 百分比] [柱状图 绝对值]

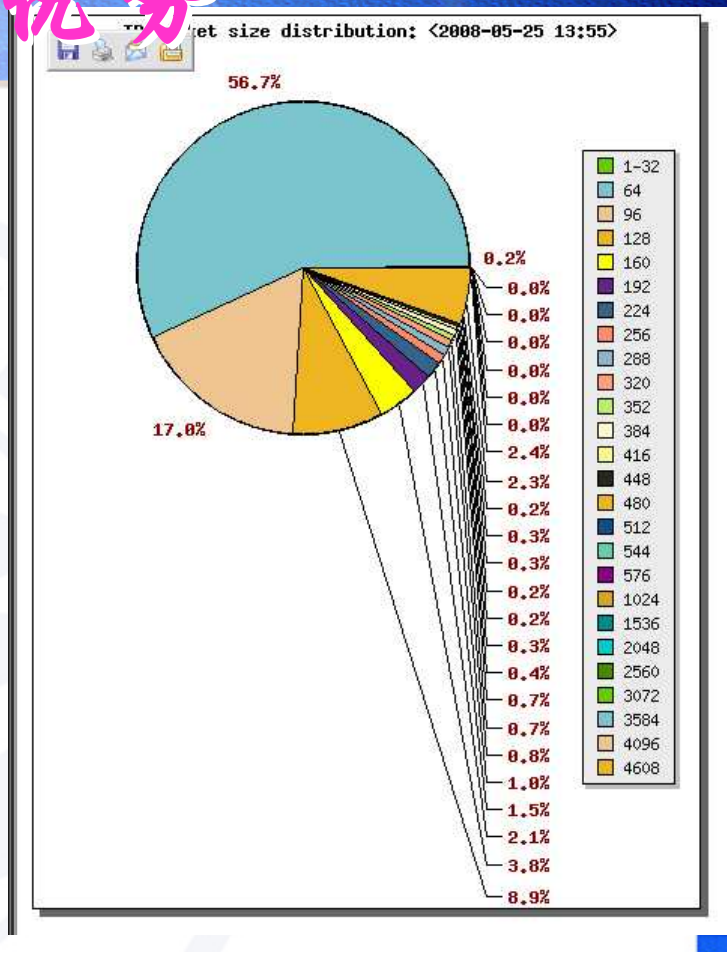
Octets per flow distribution:

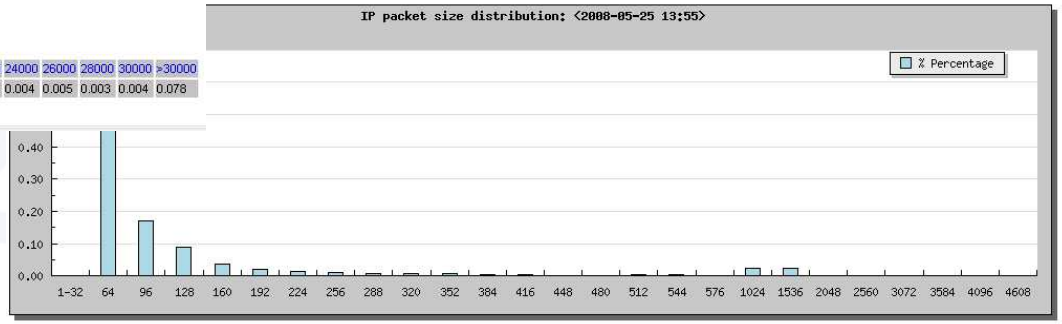
32	64	128	256	512	1280	2048	2816	3584	4352	5120	5888	6656	7424	8192	8960	9728	10496	11264	12032	12800	13568	14336	15104	15872	>15872
0.002	0.191	0.206	0.152	0.087	0.138	0.045	0.026	0.012	0.013	0.054	0.015	0.010	0.003	0.003	0.003	0.007	0.002	0.001	0.001	0.001	0.001	0.001	0.001	0.001	0.025

[饼图 百分比] [柱状图 绝对值]

Flow time distribution:

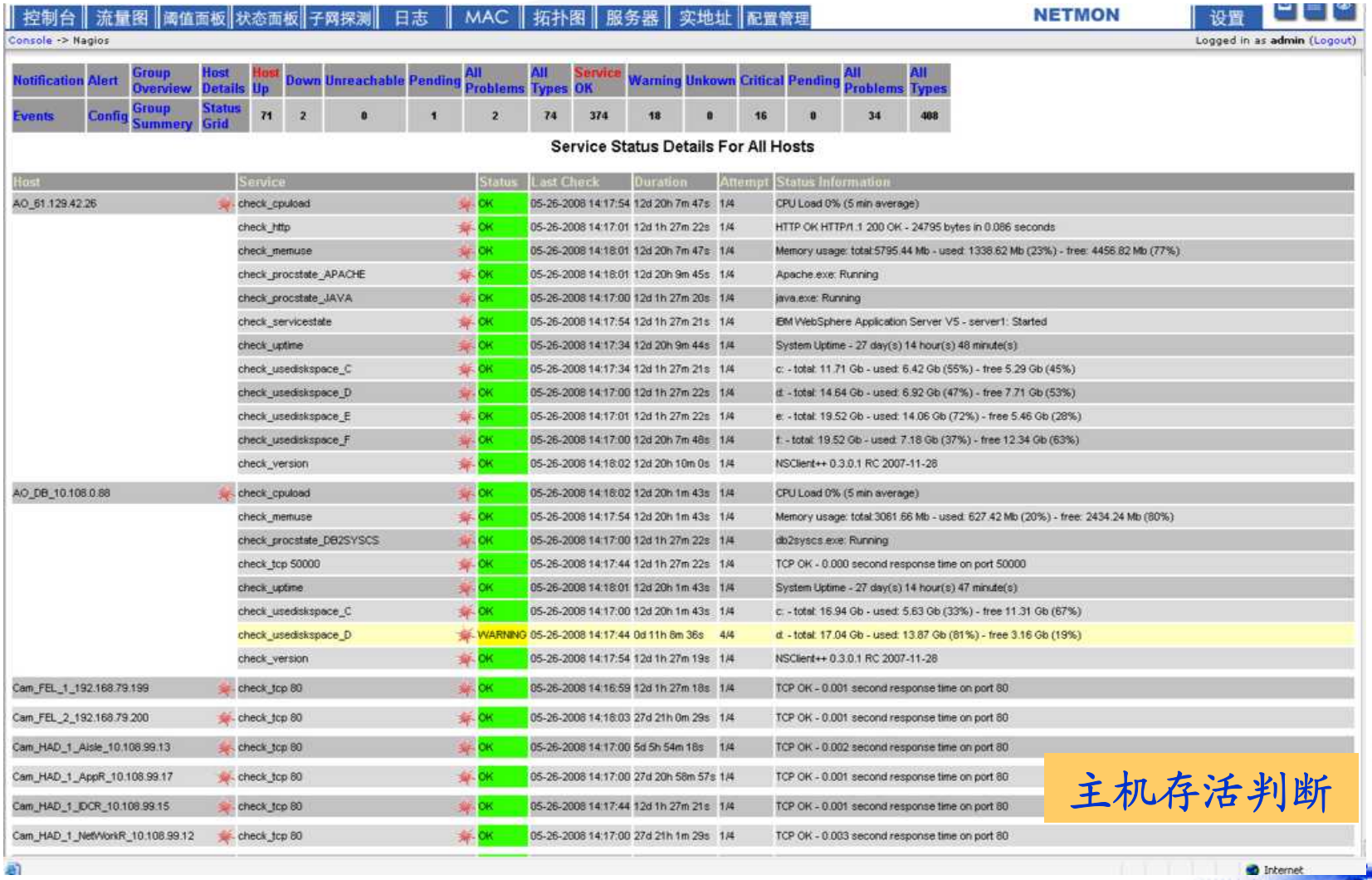
10	50	100	200	500	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000	12000	14000	16000	18000	20000	22000	24000	26000	28000	30000	>30000
0.402	0.055	0.019	0.028	0.050	0.037	0.041	0.036	0.029	0.017	0.014	0.013	0.009	0.056	0.040	0.015	0.009	0.012	0.007	0.008	0.010	0.004	0.005	0.003	0.004	0.078





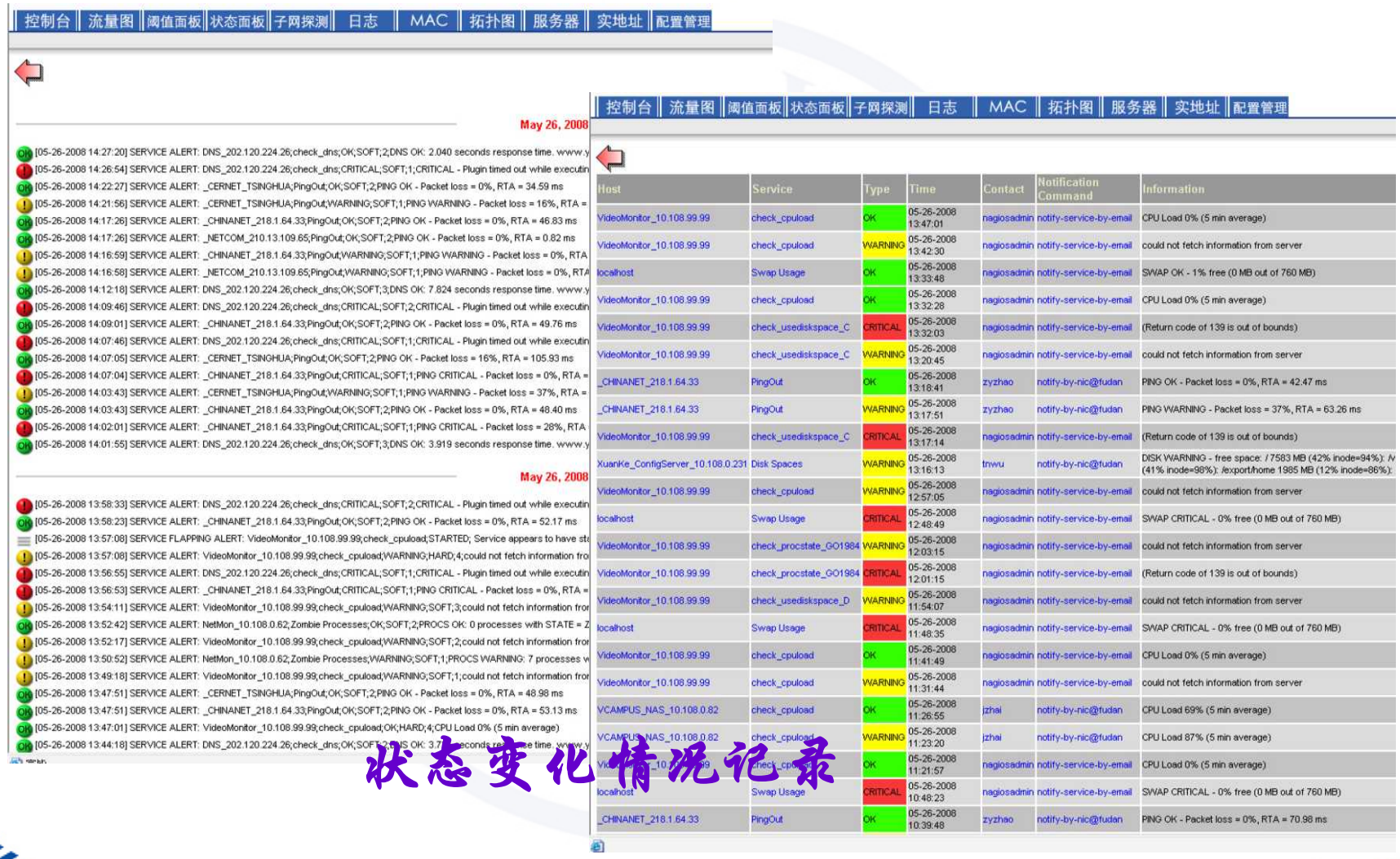
E-campus

依托技术优势



主机存活判断

依托技术优势



状态变化情况记录

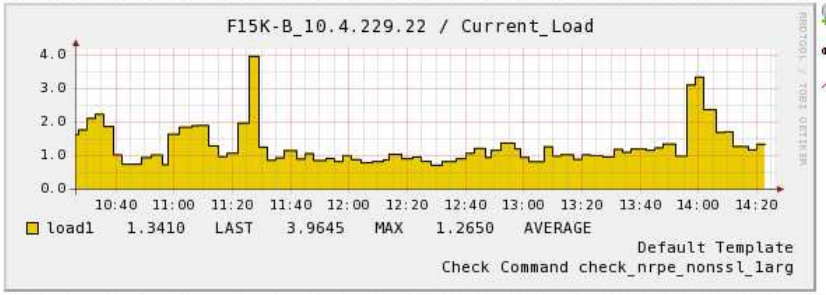
E-campus

依托技术优势

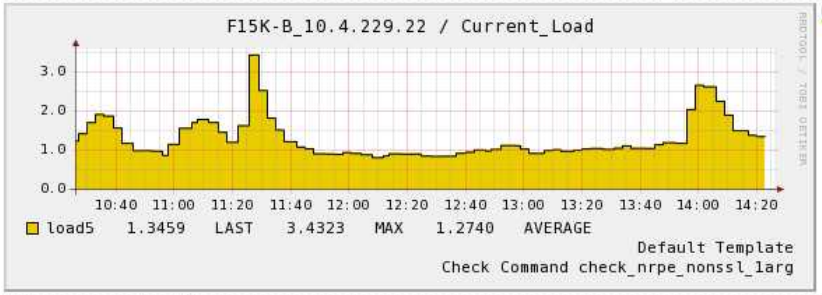
Service Overview

4 Hours (26.05.08 10:26 - 26.05.08 14:26)

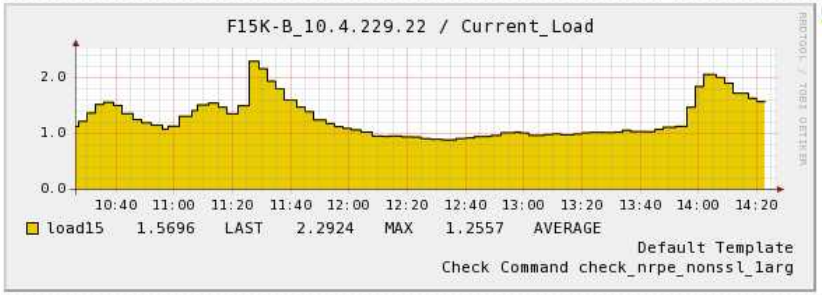
Datasource: load1



Datasource: load5



Datasource: load15



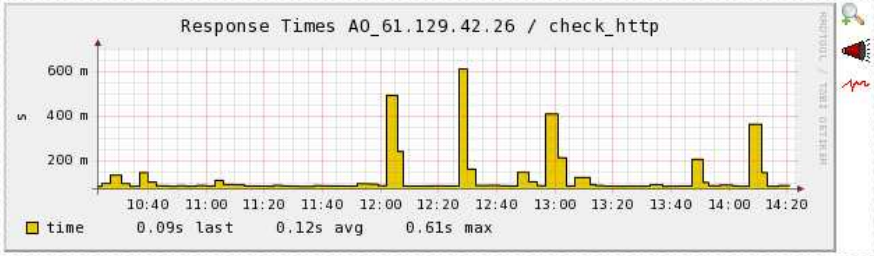
24 Hours (25.05.08 14:26 - 26.05.08 14:26)

Datasource: load1

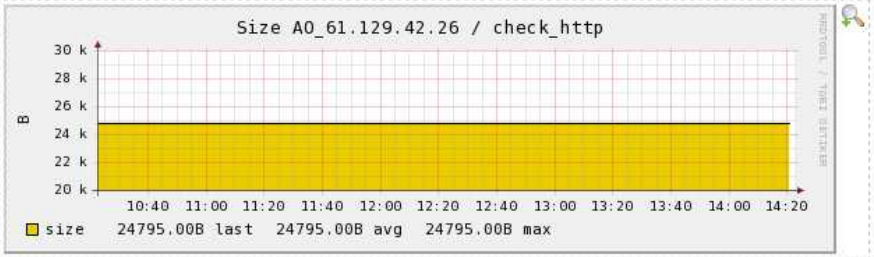
Service Overview

4 Hours (26.05.08 10:22 - 26.05.08 14:22)

Datasource: time

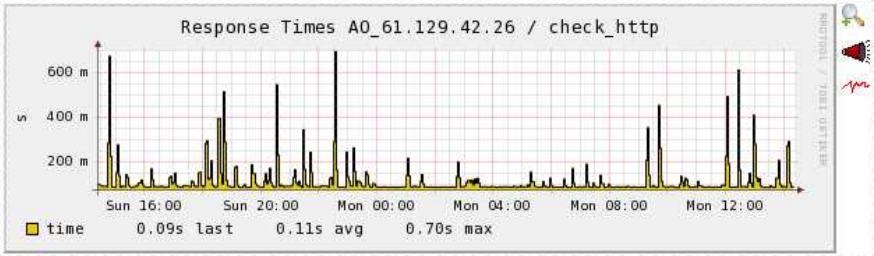


Datasource: size

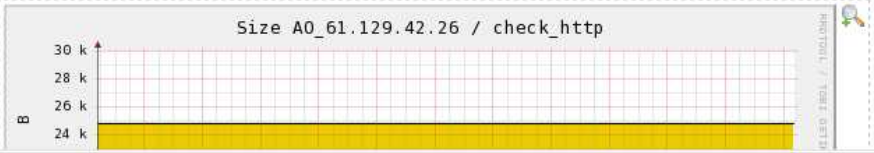


24 Hours (25.05.08 14:22 - 26.05.08 14:22)

Datasource: time

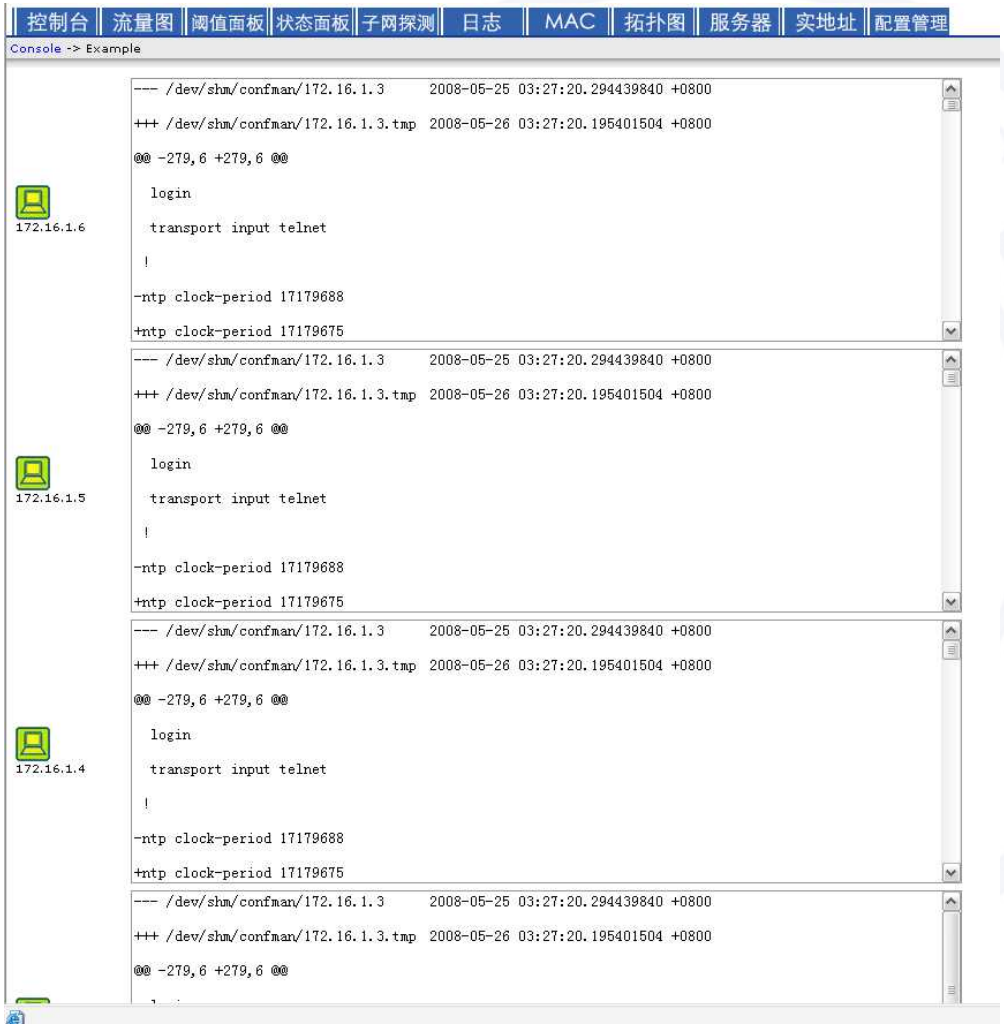


Datasource: size



E-campus

依托技术优势




```
Building configuration...

Current configuration : 75047 bytes
!
! Last configuration change at 19:11:47 CST Sun May 25 2008
! NVRAM config last updated at 16:10:28 CST Thu May 22 2008
!
version 12.2
service timestamps debug uptime
service timestamps log datetime localtime
service password-encryption
service counters max age 10
!
hostname 6509_6_guanghua
!
boot system flash sup-bootflash:
logging snmp-authfail
logging buffered 3000000 debugging
no logging console
enable secret 5 $1$XKWT$sJjUiO4LTLw4Mr.6peKhX0
!
username admin password 7 12110D0D011F1F08
no aaa new-model
clock timezone CST 8

ip subnet-zero
ip flow-cache timeout active 2
!
!
ip ftp username jliu
ip ftp password 7 070E234F1F5B4A
no ip domain-lookup
ip domain-name core
!
ip dhcp snooping vlan 240
ipv6 unicast-routing
ipv6 multicast-routing
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
mls qos
mls cef error action freeze
!
!
!
!
!
!
power redundancy-mode combined
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
redundancy
 mode sso
 main-cpu
```

E-campus

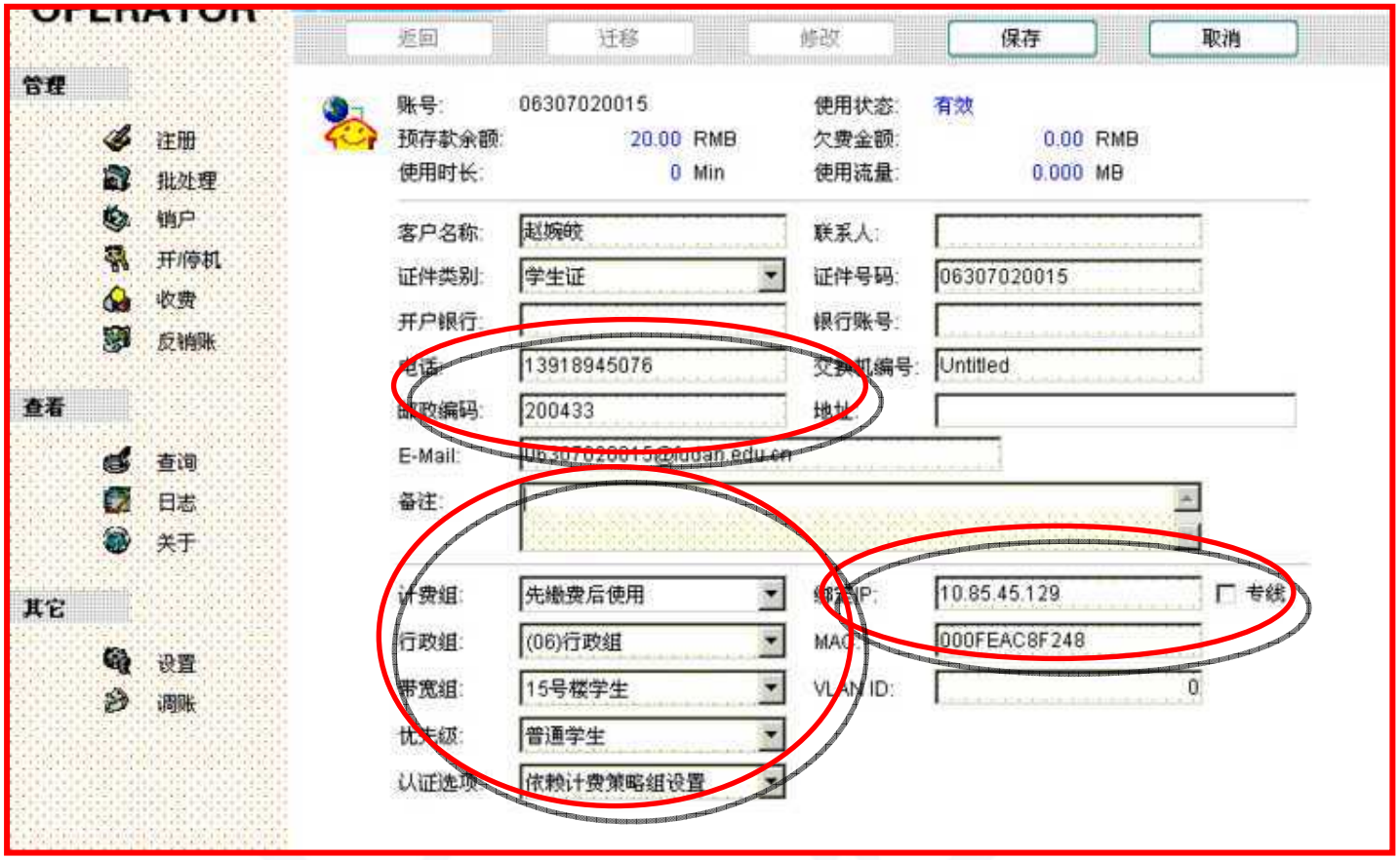
依托技术优势

- 运行日志
  - 目前收录近25台服务器/交换机的日志
  - Syslog服务器收录完整的日志
  - Netmon仅收录Err、crit、 emerg 、warning等4个级别，每天6万-8万条记录
  - Mysql数据库

Limit

	facility	priority	date	time	host	message		seq
	local0	crit	2008-05-08	19:42:08	10.220.1.13	apf_mm.c:716 APF-3-MOBIL...	99 b...	446305
	local0	crit	2008-05-08	19:42:05	10.220.1.11	iapp_socket_task.c:580 I...	83 b...	446303
	local0	crit	2008-05-08	19:42:08	10.220.1.11	apf_utils.c:333 APF-3-UN...	61 b...	446304
	local0	crit	2008-05-08	19:42:05	10.220.1.11	iapp_socket_task.c:580 I...	83 b...	446302
	local0	crit	2008-05-08	19:42:05	10.220.1.11	iapp_socket_task.c:580 I...	83 b...	446301
	local7	warning	2008-05-08	19:42:03	202.120.228.22	14295310: May 8 19:42:0...	159 b...	446300
	local7	warning	2008-05-08	19:42:03	172.16.1.5	185074l: May 8 19:42:02...	154 b...	446299
	local0	crit	2008-05-08	19:42:01	10.220.1.11	apf_utils.c:333 APF-3-UN...	61 b...	446298
	local7	warning	2008-05-08	19:42:00	HC65_2-6	1191502: May 8 19:41:59...	164 b...	446297
	local7	warning	2008-05-08	19:41:58	202.120.228.22	14295309: May 8 19:41:5...	151 b...	446296
	local0	crit	2008-05-08	19:41:56	10.220.1.11	apf_utils.c:333 APF-3-UN...	61 b...	446295
	local0	crit	2008-05-08	19:41:55	10.220.1.15	iapp_socket_task.c:580 I...	83 b...	446294

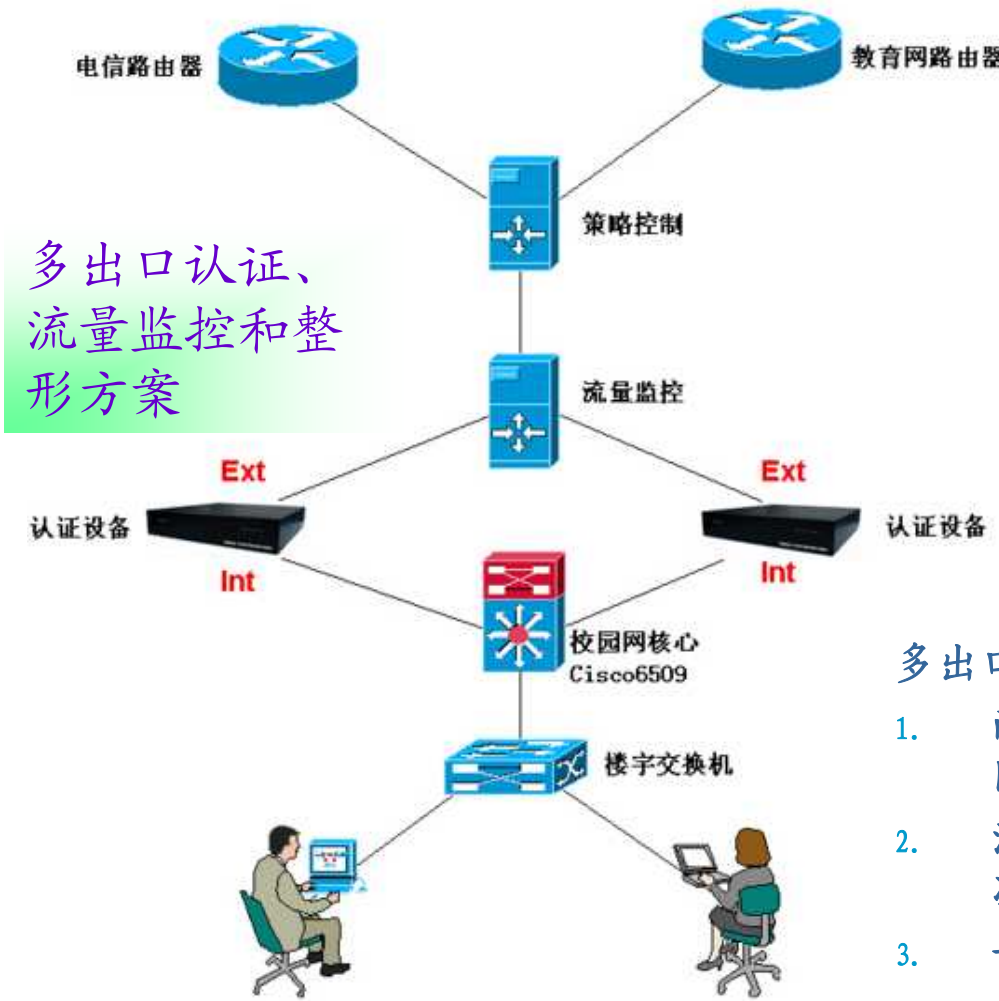
依托技术优势

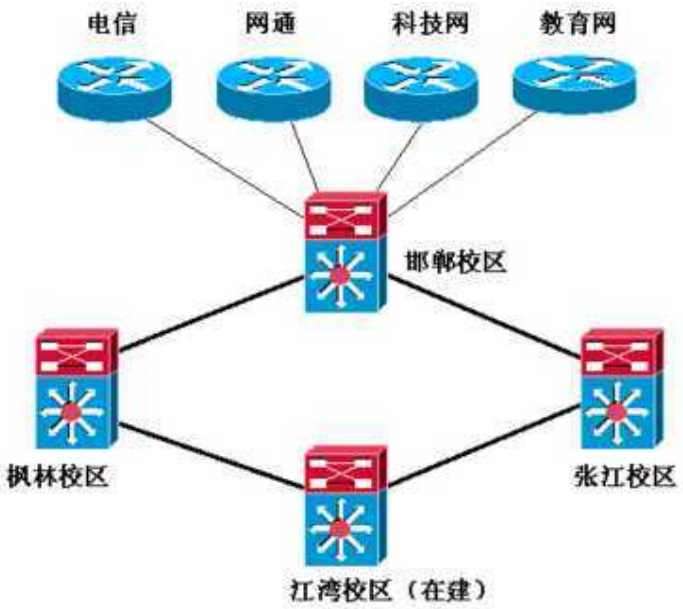


上网实名登记、绑定IP和MAC地址，减少安全隐患

依托技术优势

多出口认证、流量监控和整形方案

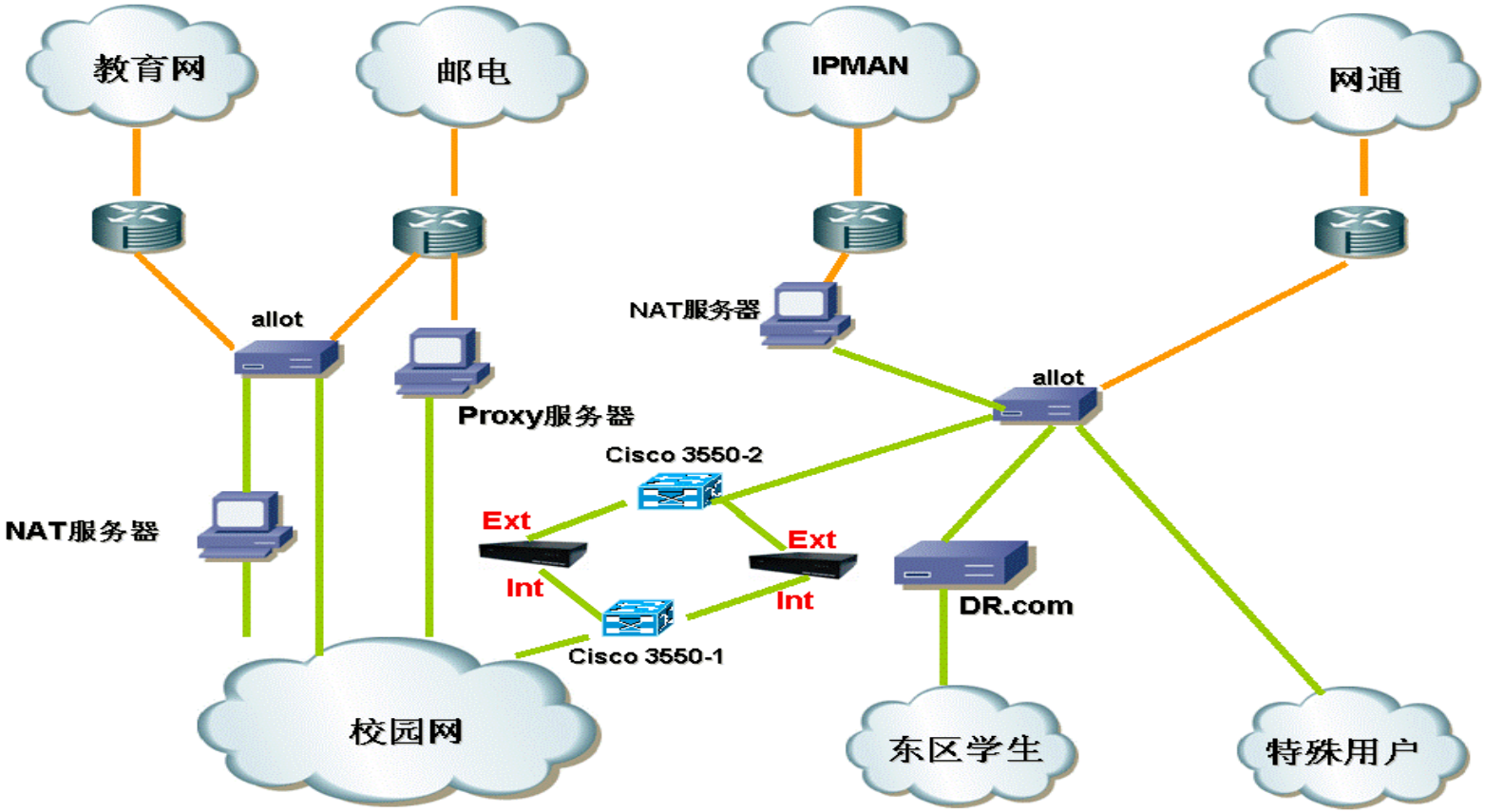




多出口路由

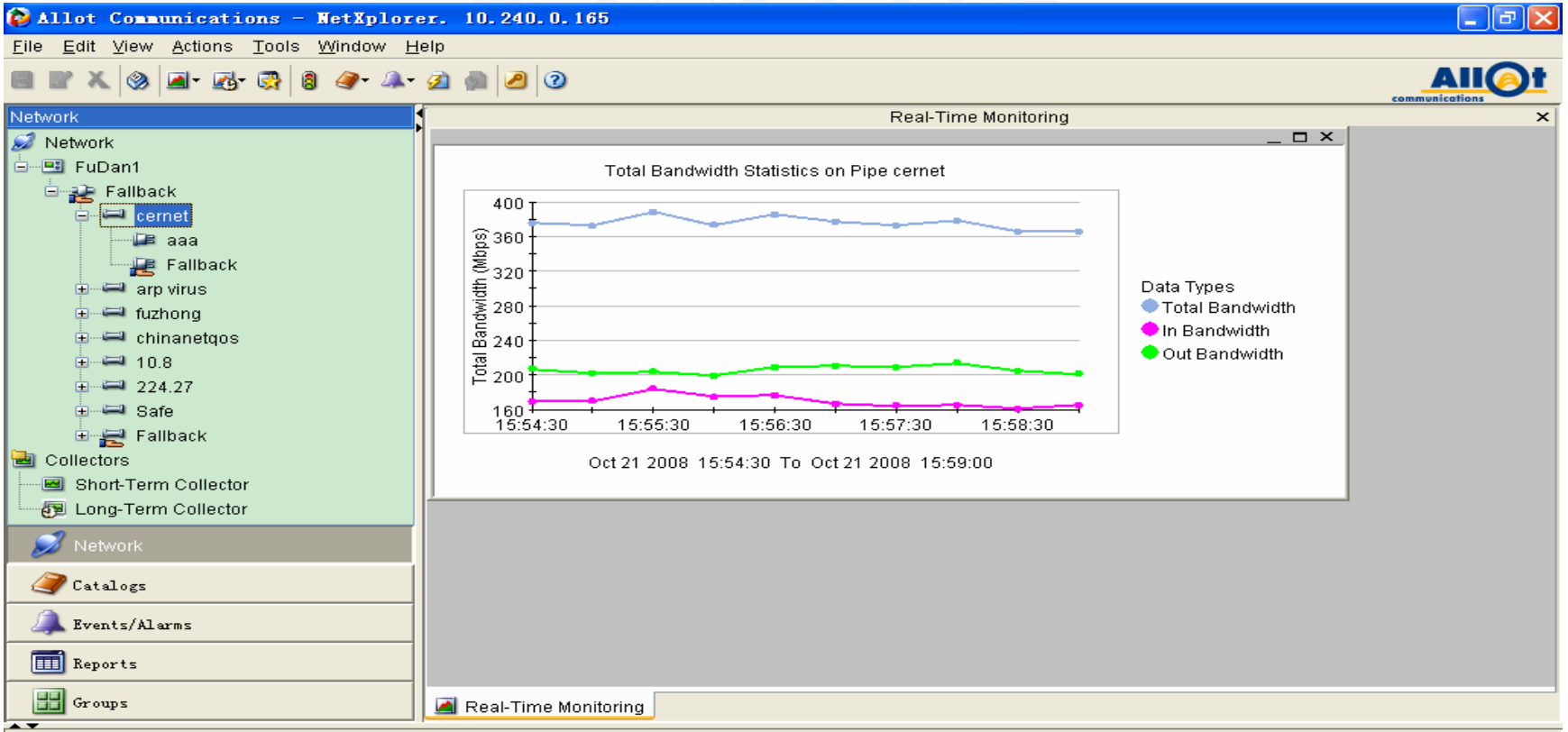
1. 两台城市热点设备互为热备负责用户上网认证和用户访问情况的记录
2. 流量整型设备负责流量整型和对流量情况进行实时监控
3. 一台路由器负责配置策略
4. 出口路由器配置GLBP+SLA配合NAT实现多出口路由的自动切换和负责均衡

依托技术优势


教育网
邮电
IPMAN
网通
allot
NAT服务器
Proxy服务器
allot
Cisco 3550-2
NAT服务器
Ext
Ext
Int
Int
DR.com
Cisco 3550-1
校园网
东区学生
特殊用户

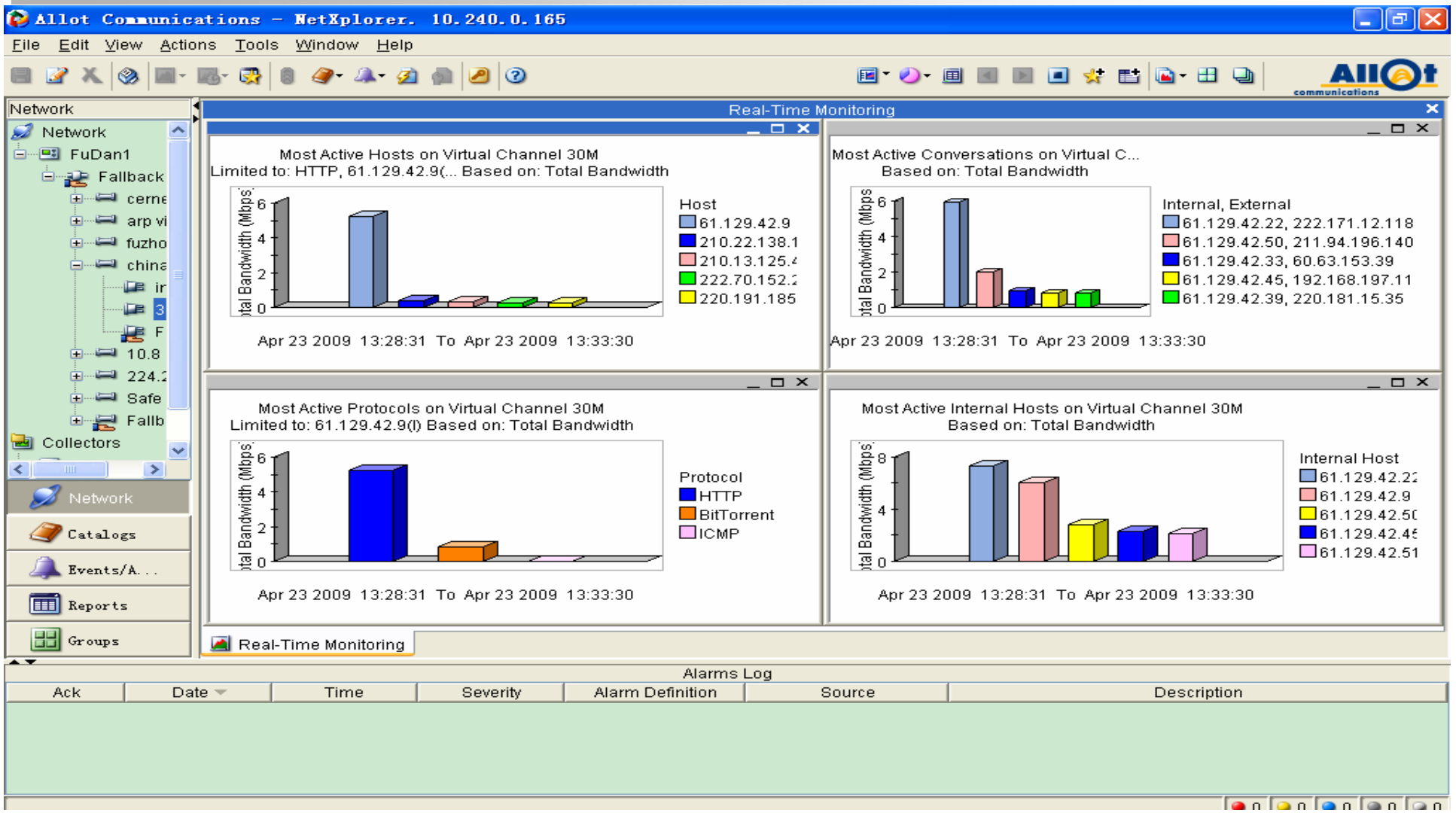
依托技术优势

使用专业的网络流量管理硬件设备做流量的监视和控制 **ALLOT流量监控**



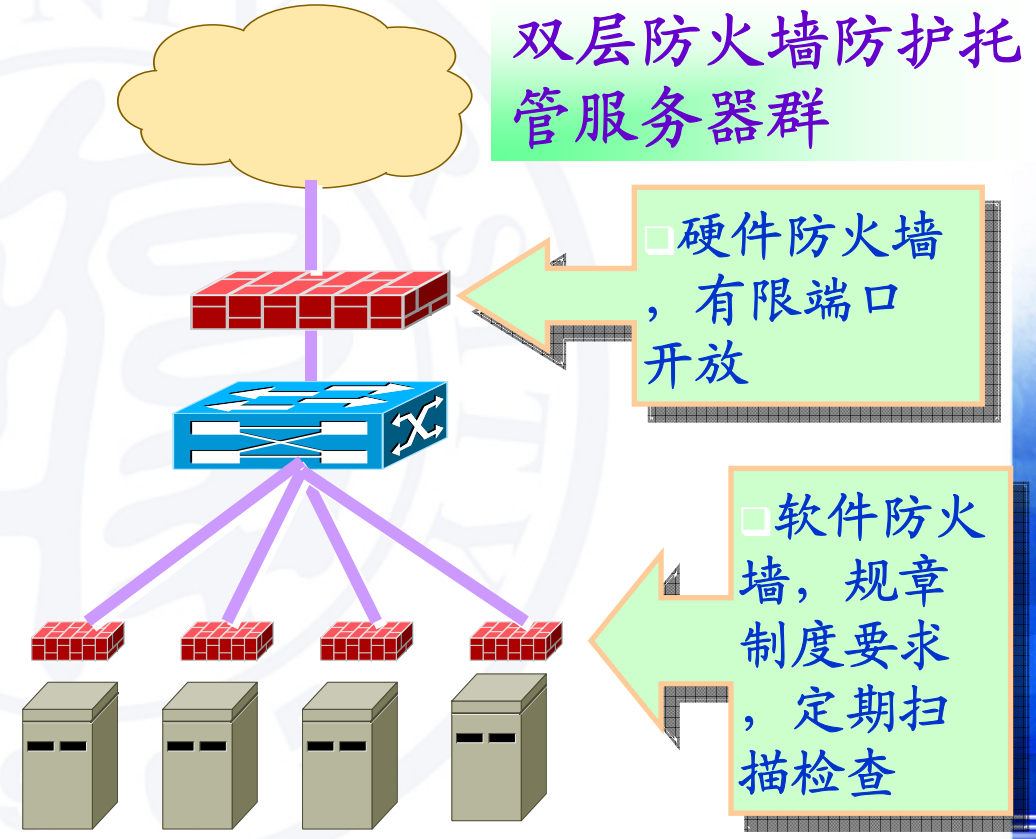
依托技术优势

使用专业的网络流量管理硬件设备做流量的监视和控制 **ALLOT流量监视**



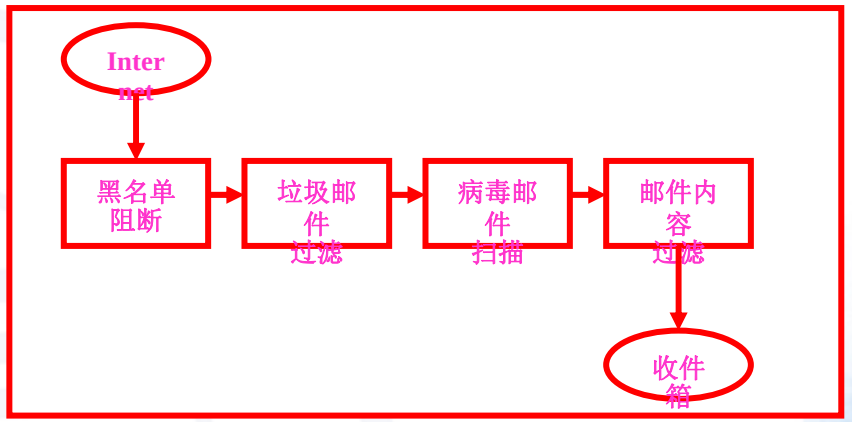
依托技术优势

- 规划专用服务器网段，双层防火墙防护
- 二级域名服务用反向代理
  - 避免服务器与外界直接接触
- 定期漏洞扫描，结果通报管理员
- 日志服务器
  - UNIX标准syslog，实现日志实时备份
  - Solaris、Linux服务器
  - 交换机、路由器



依托技术优势

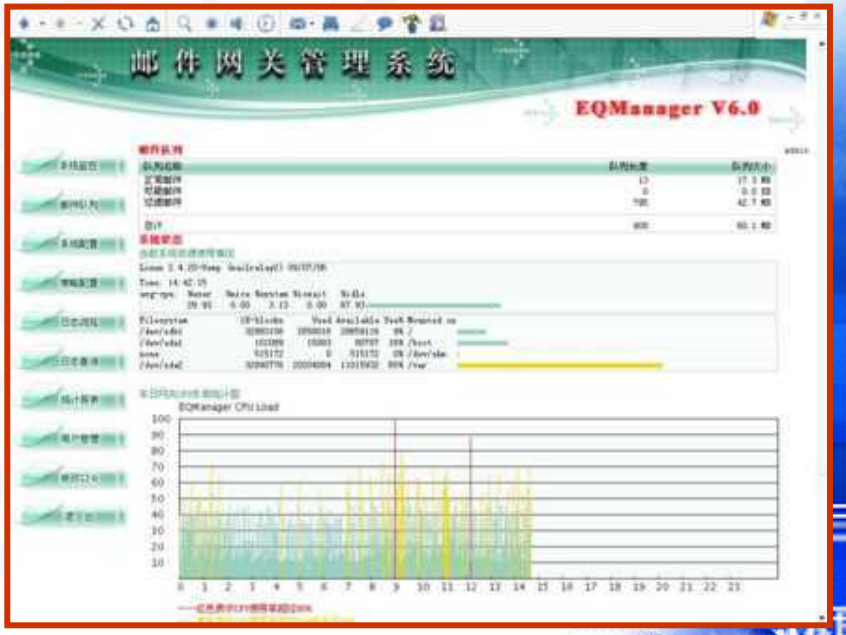
- 邮件网关：过滤垃圾邮件
- 响应制度：根据用户举报，分析垃圾邮件特征并设置过滤规则



从	0356141@fudan.edu.cn
已发送	星期日，九月 3日，2006 下午10:17
收件人	nic@fudan.edu.cn
抄送	
密件抄送	
主题	转发:网赚信息网成立了（垃圾邮件举报）

----- 原邮件 -----
从 opnrisg <opnrisgwxynwv@alibaba.com>
日期 Fri, 01 Sep 2006 09:35:29 +0800
收件人 0356141 <0356141@fudan.edu.cn>
主题 网赚信息网成立了

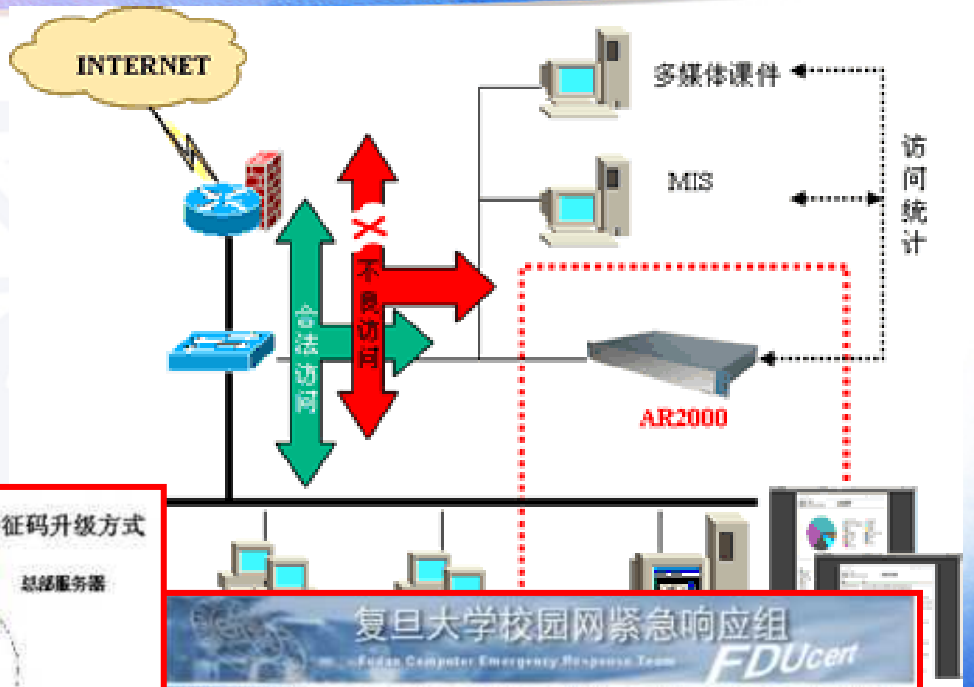
您好：

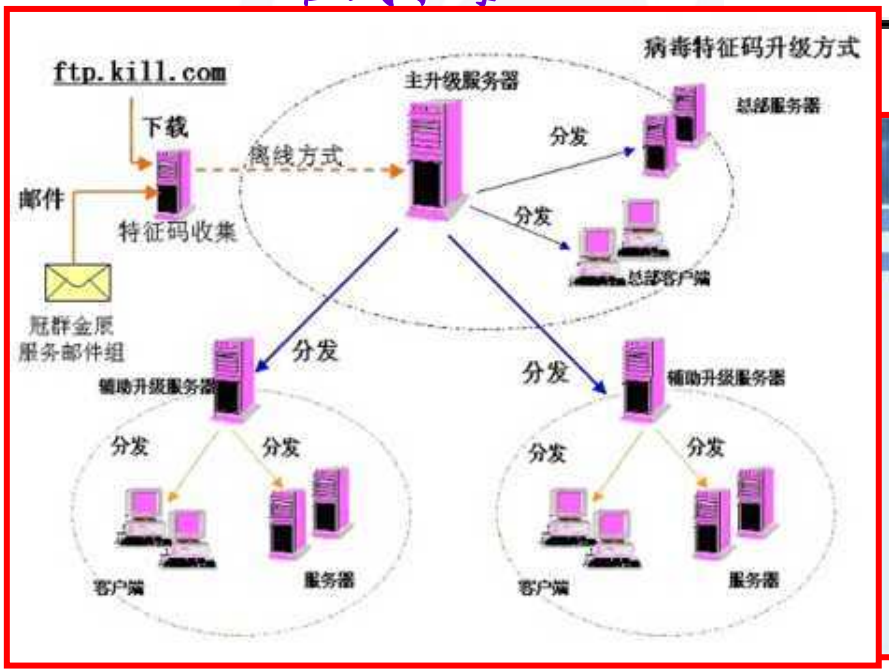


E-campus

依托技术优势

- 信息过滤：利用旁路监听技术，过滤不良网络访问
- 杀毒软件
  - 单机版
  - 网络版
    (卡巴斯机、赛门铁克）
  - 在线杀毒

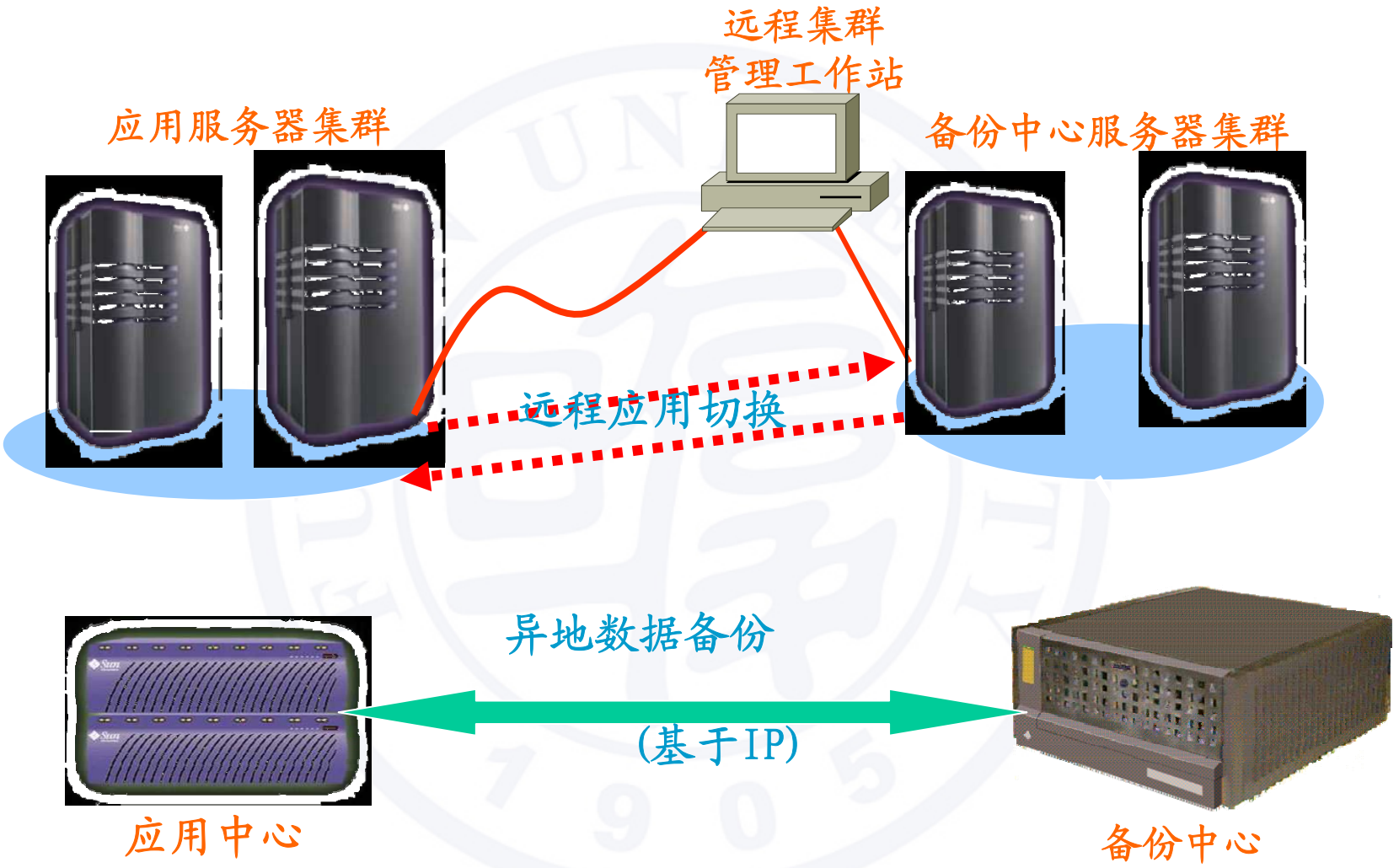




依托技术优势

- CERT
- WSUS
- 日志服务器

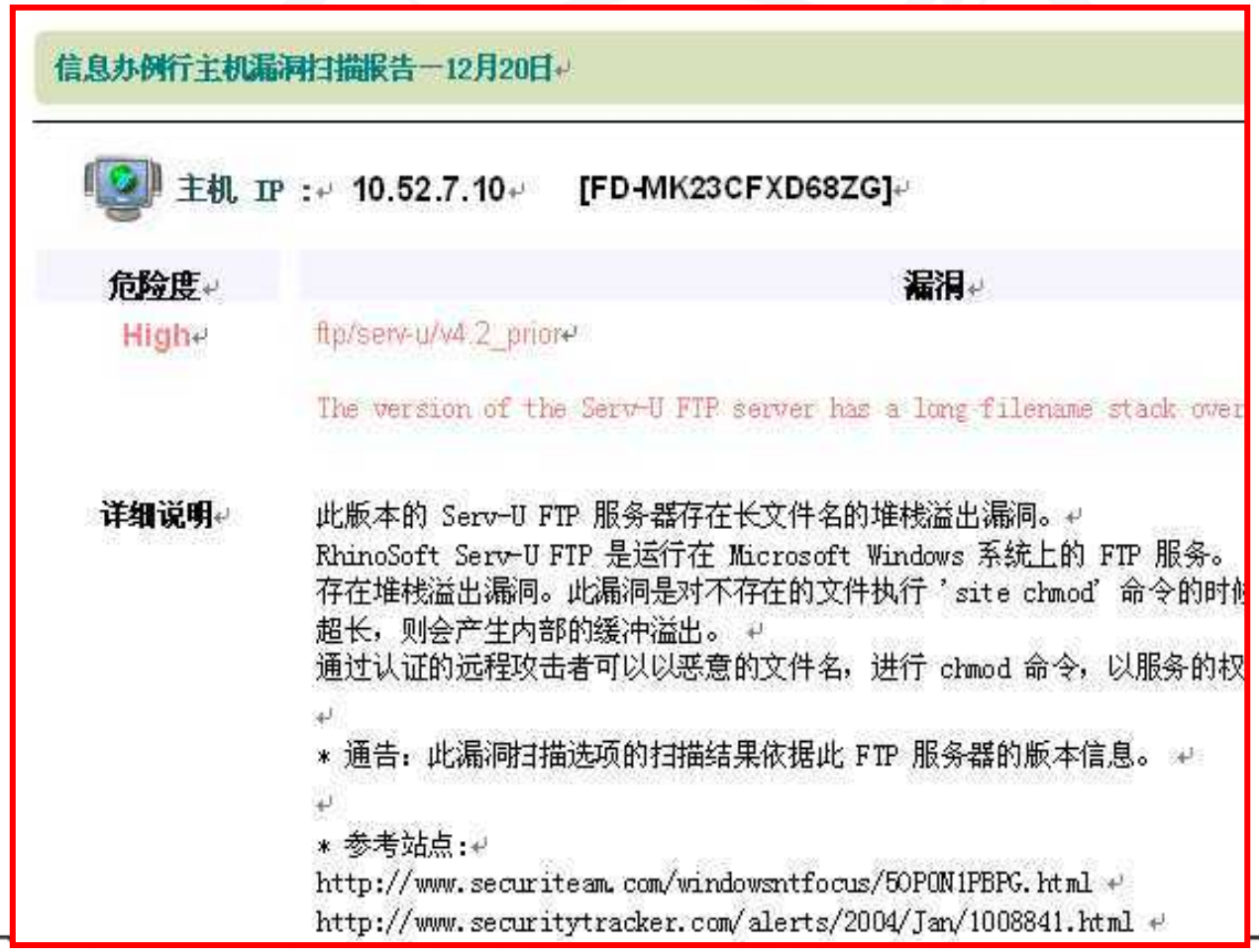
依托技术优势



系统备份容灾方案示意图

依托技术优势

- 规范托管服务器管理行为，不达标的不准上架
- 定期进行漏洞扫描(冠群金辰－辰影)，生成报告通知网站管理员，并强制整改



信息办例行主机漏洞扫描报告—12月20日

主机 IP：10.52.7.10 [FD-MK23CFXD68ZG]

危险度	漏洞
High	ftp/serv-u/v4.2_prior
	The version of the Serv-U FTP server has a long filename stack over

详细说明

此版本的 Serv-U FTP 服务器存在长文件名的堆栈溢出漏洞。
RhinoSoft Serv-U FTP 是运行在 Microsoft Windows 系统上的 FTP 服务。
存在堆栈溢出漏洞。此漏洞是对不存在的文件执行 'site chmod' 命令的时
超长，则会产生内部的缓冲溢出。
通过认证的远程攻击者可以以恶意的文件名，进行 chmod 命令，以服务的权

* 通告：此漏洞扫描选项的扫描结果依据此 FTP 服务器的版本信息。

* 参考站点：
http://www.securiteam.com/windowsntfocus/5OPON1PBPG.html
http://www.securitytracker.com/alerts/2004/Jan/1008841.html

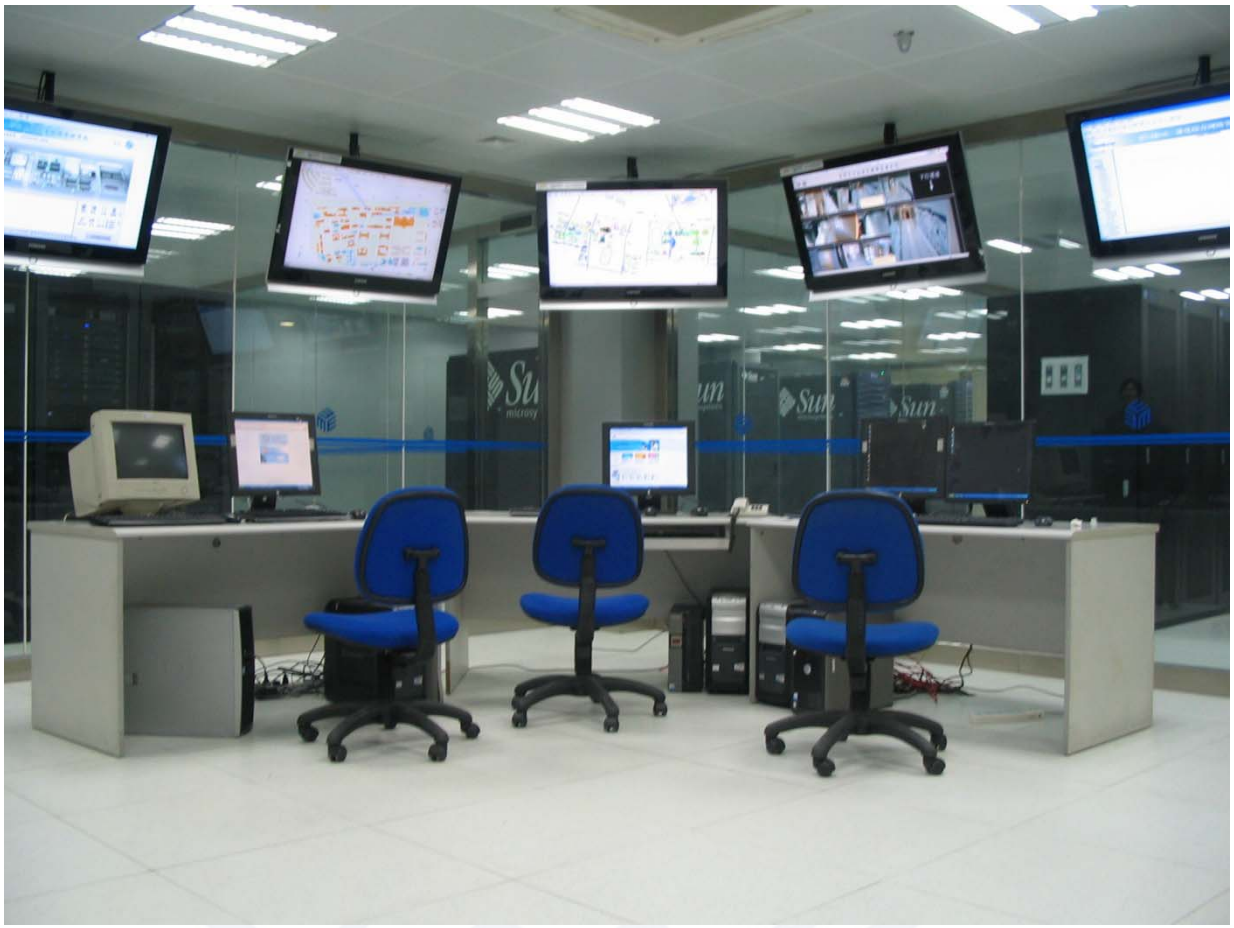
机房与环境建设

- 机房动力监控 1套
- 提供365*24小时的烟感、漏水、温湿度检测和报警

机房与环境建设

- 视频监控
- 全天候视频监视和动态图像记录

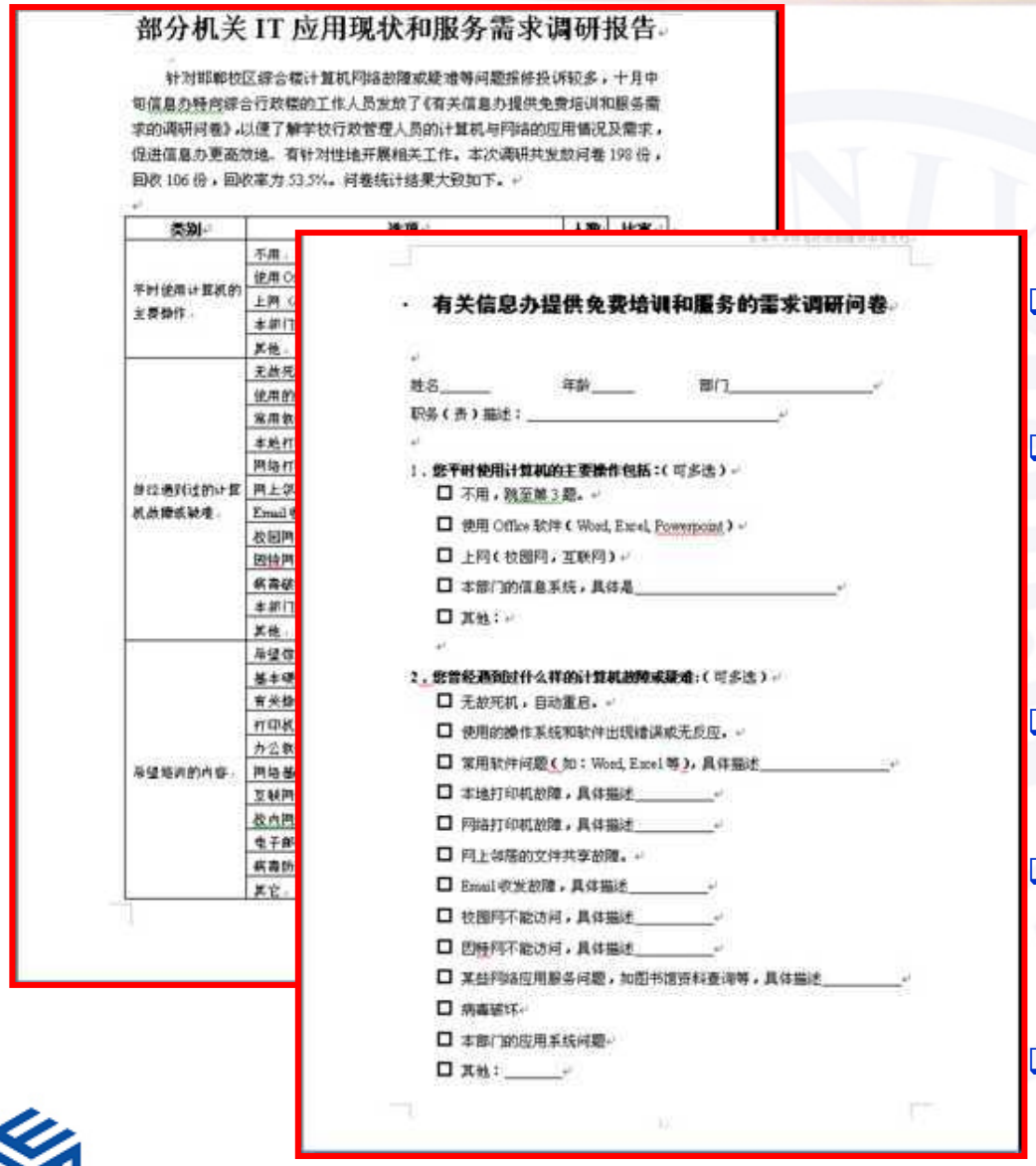
机房与环境建设



网管监控室：5块40”液晶显示屏

实时进行网络监控、机房动力监控和视频监控

开展用户培训



部分机关 IT 应用现状和服务需求调研报告

针对邯郸校区综合楼计算机网络故障或疑难等问题报修投诉较多，十月中旬信息办特向综合行政楼的工作人员发放了《有关信息办提供免费培训和服务需求的调研问卷》，以便了解学校行政管理人员的计算机与网络的应用情况及需求，促进信息办更高效地、有针对性地开展相关工作。本次调研共发放问卷 198 份，回收 106 份，回收率为 53.5%。问卷统计结果大致如下。

类别	选项	人数	比率
平时使用计算机的主要操作	不用		
	使用 Office 软件（Word, Excel, Powerpoint）		
	上网（校园网，互联网）		
	本部门的信息系统，具体是		
	其他		
曾经遇到过的计算机故障或疑难	无故死机，自动重启		
	使用的操作系统和软件出现错误或无反应		
	常用软件问题（如：Word, Excel 等），具体描述		
	本地打印机故障，具体描述		
	网络打印机故障，具体描述		
	网上邻居的文件共享故障		
	Email 收发故障，具体描述		
	校园网不能访问，具体描述		
	因特网不能访问，具体描述		
	某些网络应用服务问题，如图书馆资料查询等，具体描述		
	病毒破坏		
	本部门的应用系统问题		
	其他		
希望培训的内容	基本硬件		
	有关软件		
	打印机		
	办公软件		
	网络基础		
	互联网		
	校内网		
	电子邮件		
	病毒防治		
	其它		

· 有关信息办提供免费培训和服务的需求调研问卷

姓名_____ 年龄_____ 部门_____

职务（责）描述：_____

1．您平时使用计算机的主要操作包括：（可多选）

- ☐ 不用，跳至第 3 题。
- ☐ 使用 Office 软件（Word, Excel, Powerpoint）
- ☐ 上网（校园网，互联网）
- ☐ 本部门的信息系统，具体是_____
- ☐ 其他：

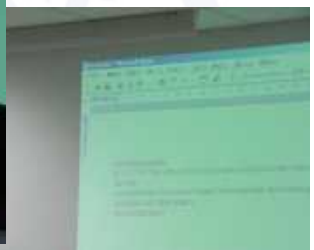
2．您曾经遇到过什么样的计算机故障或疑难：（可多选）

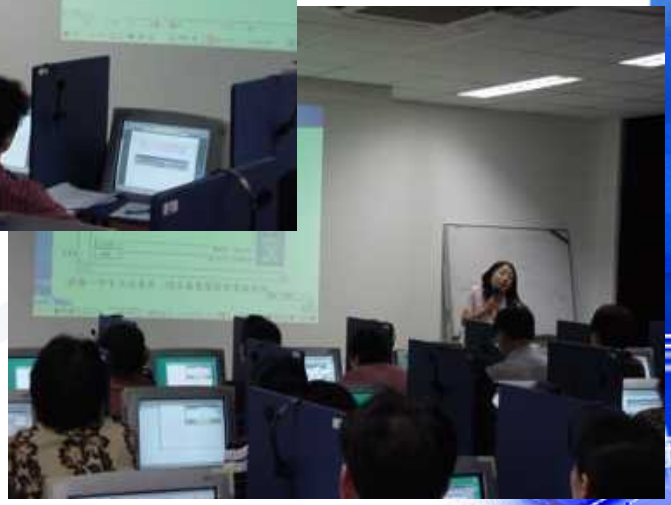
- ☐ 无故死机，自动重启。
- ☐ 使用的操作系统和软件出现错误或无反应。
- ☐ 常用软件问题（如：Word, Excel 等），具体描述_____
- ☐ 本地打印机故障，具体描述_____
- ☐ 网络打印机故障，具体描述_____
- ☐ 网上邻居的文件共享故障。
- ☐ Email 收发故障，具体描述_____
- ☐ 校园网不能访问，具体描述_____
- ☐ 因特网不能访问，具体描述_____
- ☐ 某些网络应用服务问题，如图书馆资料查询等，具体描述_____
- ☐ 病毒破坏
- ☐ 本部门的应用系统问题
- ☐ 其他：_____

为促进师生信息化应用水平的提高、配合信息化应用项目的推广和改善信息化应用环境，结合学校实际情况，对师生、行政人员开展有针对性的培训工作。

- 计算机能力培训：
  - 分四个班，对行政机关和院系行政人员250余人培训
- OA系统、URP系统培训：
  - 对校领导、各机关部处长、院系党政领导及部门院系的秘书进行了分批分层次（13个班、400多人次）培训 + 定期常规化培训
- 网站管理员培训
  - 操作系统安全管理、动态网页代码编写安全等
- 安全知识讲座
  - 面向校园师生不定期组织的安全知识讲座，以宣传和提高计算机安全知识水平为目的
- 内部培训
  - 针对内部服务人员进行的计算机安全培训

培训现场





E-campus

谢 谢!

E-campus