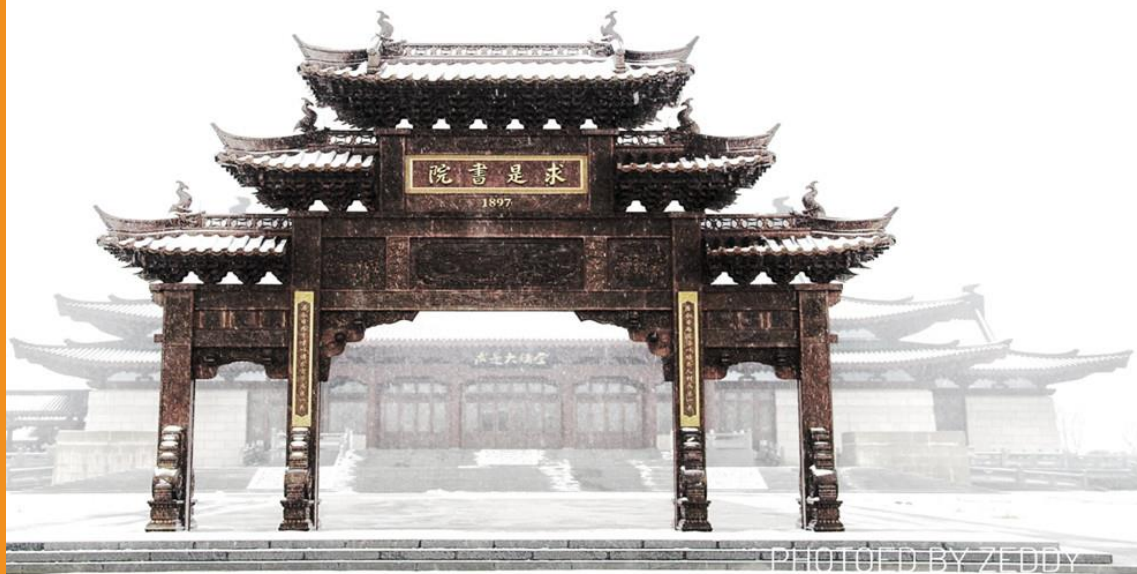


浙江大学校园网络 管理运行情况

郭晔
浙江大学信息技术中心



PHOTOED BY ZEDDY



/01

总体概况



◆ 校园网连接7大校区和7家附属医院

紫金港校区、玉泉校区、西溪校区、华家池校区、之江校区、舟山校区和海宁校区

◆ 五校区间自建光缆80公里

1998年四校合并后，学校启动自建五个校区间光缆，总长度80公里，校区内光缆360公里。

◆ 核心网络

校园网出口总带宽97G，建成20G校区互联核心网络。

◆ 接入网络

有线网络11万端口，千兆或百兆到桌面；
无线网教学区+宿舍区覆盖（AP数1万到4万升级中）



◆ 用户服务体系：

7x24小时监控咨询服务（一线团队8人）

7x8小时上门维护服务（二线团队15人）

◆ 核心服务体系

由用户服务部+系统工程部两个部门核心人员

AB角负责制

◆ 多种服务方式：

服务电话：0571-87951669

微信公众号：浙江大学信息技术中心

服务邮箱：xwmaster@zju.edu.cn



自助报障界面



一线人员受理咨询报障界面



全程监控故障单处理界面

用户服务全过程的运维管理系统

03

校园网络用户情况

◆ 校园网络账户

校园网络正常账户数约8万个

◆ 有线网络用户

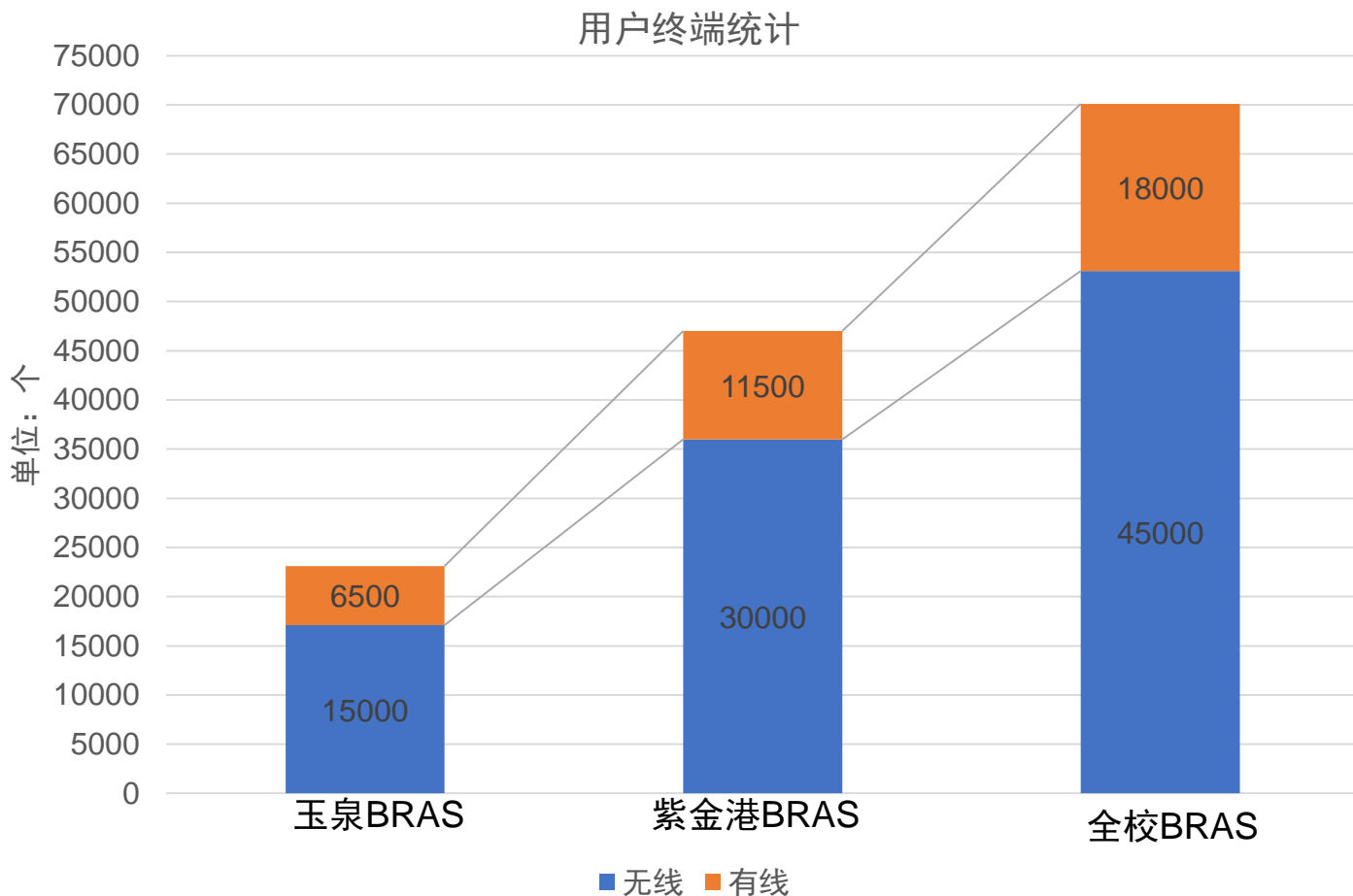
峰值在线并发终端数约1.8万个

◆ 无线网络用户

峰值在线并发终端数约4.5万个

◆ 校外接入用户

峰值在线并发终端数约4000个



◆出口带宽情况

34.6G (2018年4月) 扩容至97.2G (2019年10月)

其中CERNET从2.6G扩容至5.2G

2019年9月CERNET带宽扩容前, 带宽使用率已达92%

◆有线网络出口带宽

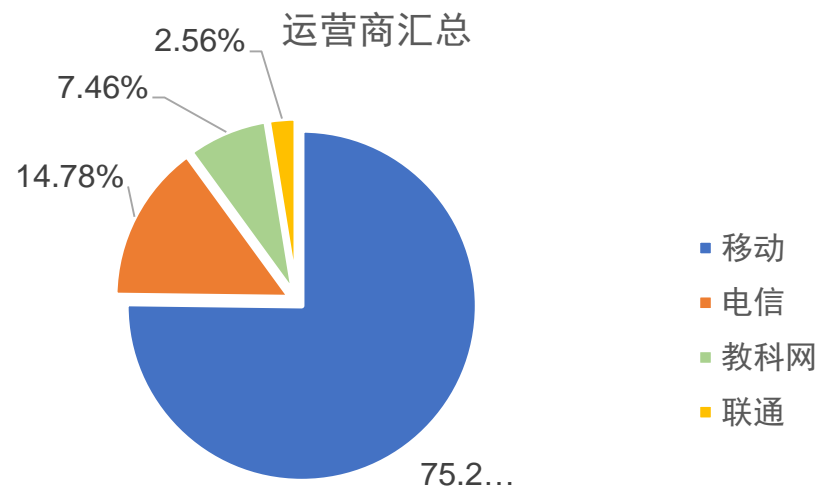
目前有线网络出口峰值带宽为16.5G

◆无线网络出口带宽

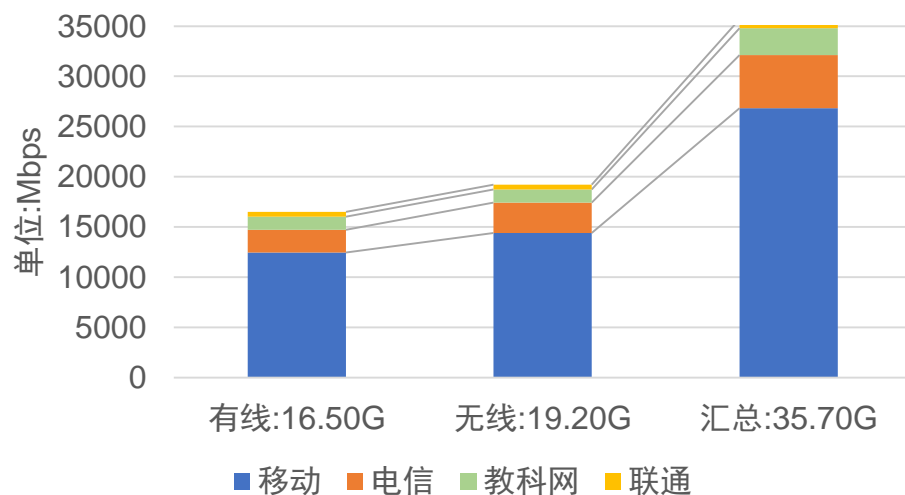
目前无线网络出口峰值带宽19.2G

◆出口带宽使用率

目前出口带宽使用率约为38%, 本学期末用户提速, 使用率提升至50%左右, 最大峰值出口带宽45G。



流量汇总



自建智能DNS域名解析系统

更高效 更安全 更稳定 无劫持

基于开源软件，浙大自主建设

日常管理 **4500** 条域名记录

每秒处理 **10000** 次用户请求

每天产生 **85 G** 日志数据

对外开放 **457** 个备案域名

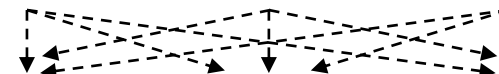
负载均衡



权威服务



跨校区多出口智能选路



递归服务



出口链路



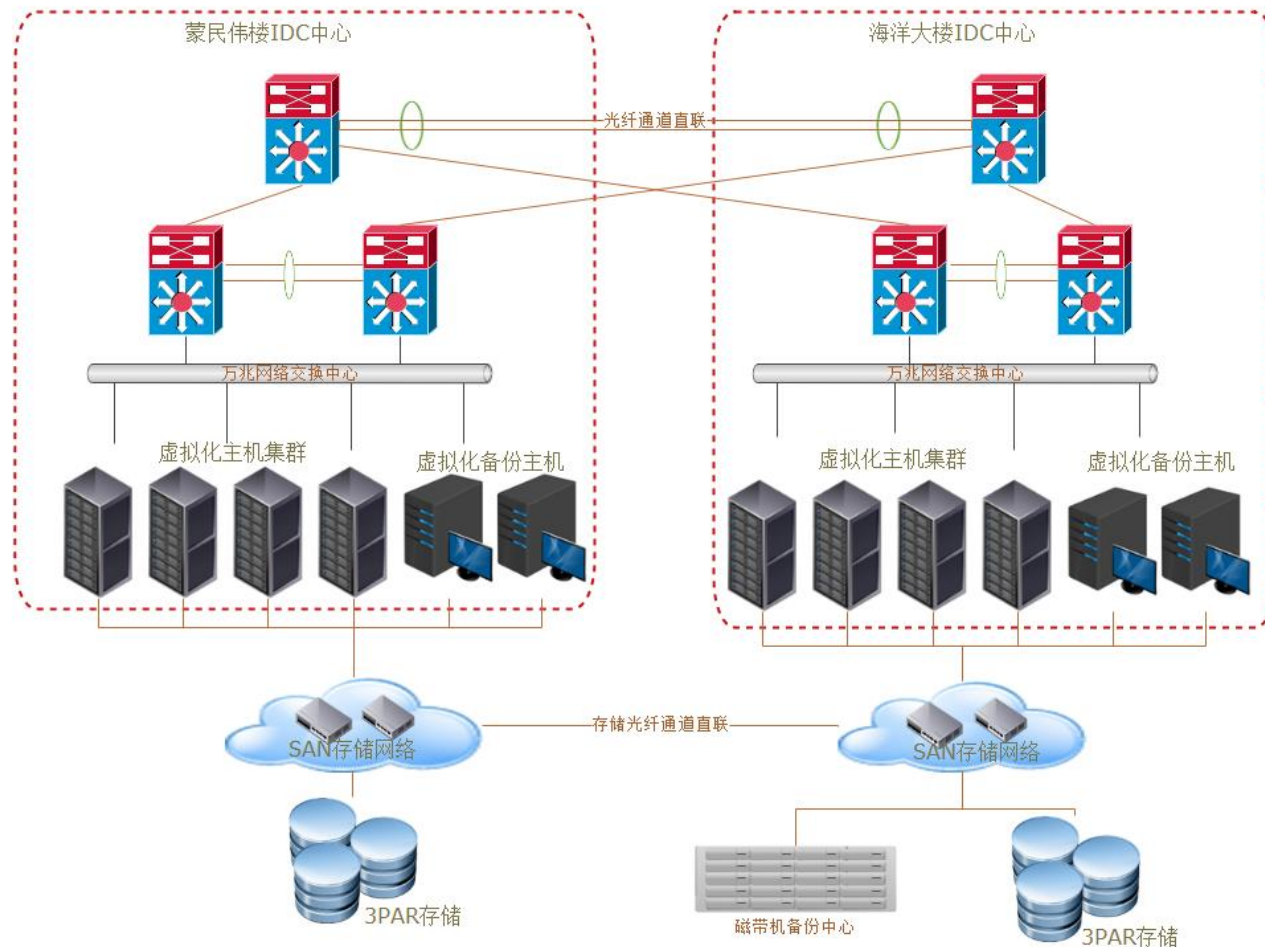
向全校提供虚拟机服务

校内其他部门逐步减少物理服务器采购，全校信息基础设施集中化

开设vm主机 900 多台

集群总内存 10T

存储容量 3PB



由96台服务器组成，提供840核、4TB内存、3.5PB存储的阿里飞天专有云集群

浙大与阿里云战略合作，致力于打造资源、应用、服务整合的**专有云平台**

并逐步向服务科研用户的**科研云**转型

已服务29个信息化项目与科研项目



浙江大学 专有云平台
ZHEJIANG UNIVERSITY



浙江大学
ZHEJIANG UNIVERSITY

浙江省高校CERNET接入情况

◆ CERNET接入情况:

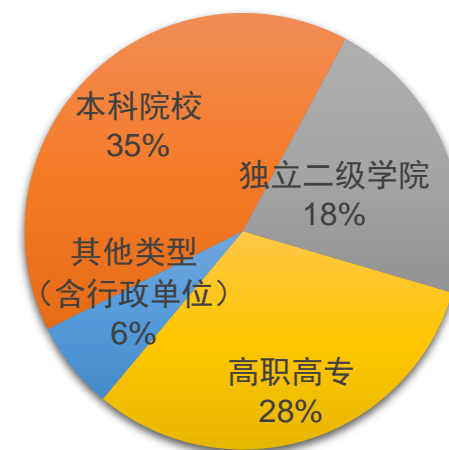
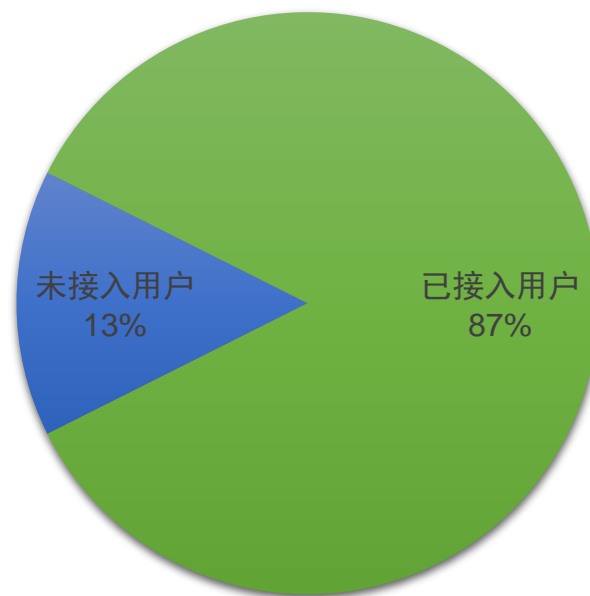
浙江省高校共108所，其中已接入94所，接入率87%

◆ 接入院校分类统计:

本科院校（含独立二级学院）58所

高职高专30所

其他类型6所



■ 未接入用户 ■ 本科院校 ■ 独立二级学院 ■ 高职高专 ■ 其他类型 (含行政单位)

浙江省高校单位接入拓扑

接入线路

省内节点和杭州市内高校通过各运营商裸纤、传输等方式接入

路由协议

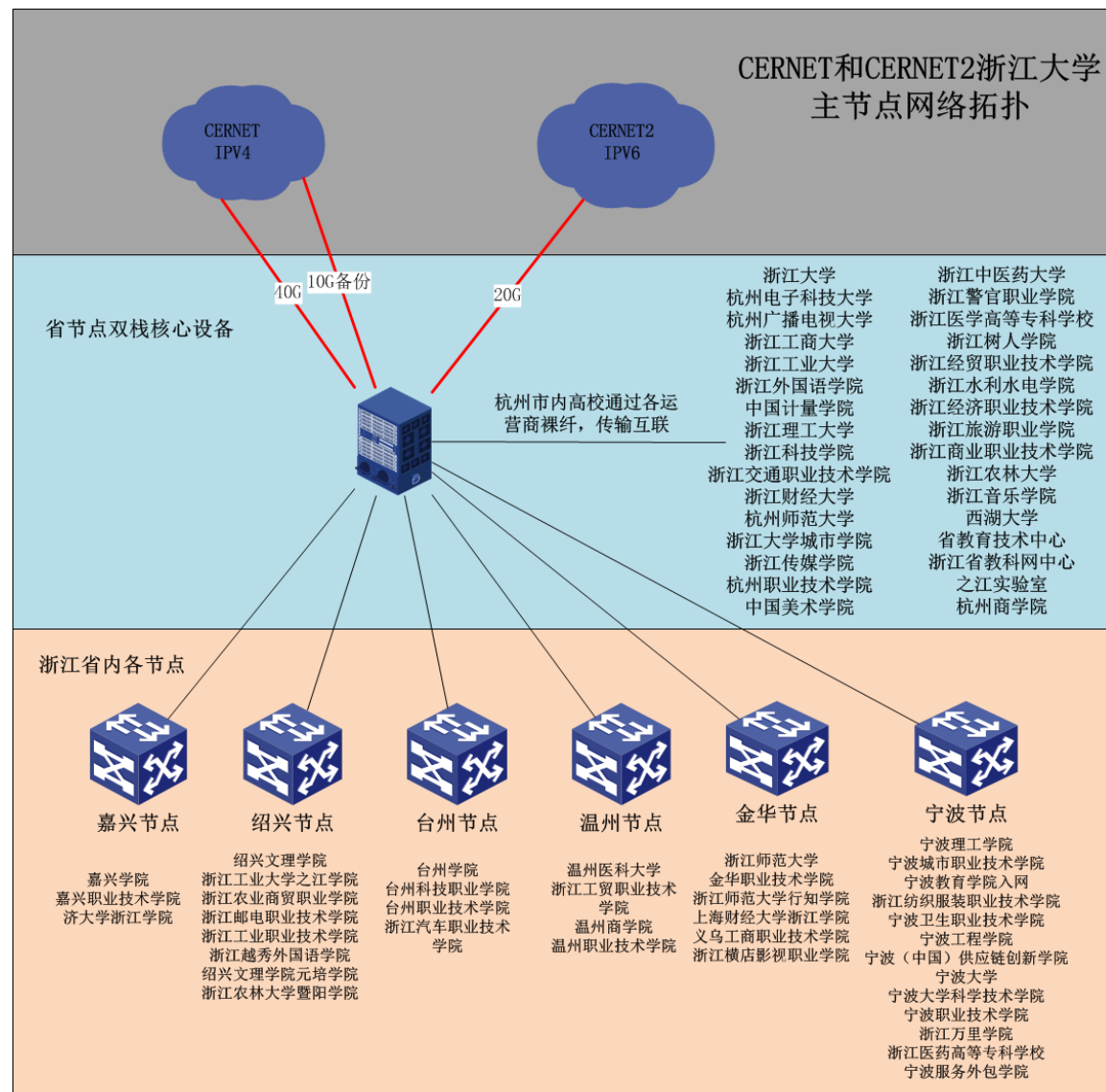
CERNET和CERNET2静态路由
省内节点和杭州市内高校静态路由
部分高校使用OSPF+OSPFv3协议
支持IPv6/IPv4双栈

冗余性

部分高校双路由裸光纤，动态路由或链路聚合

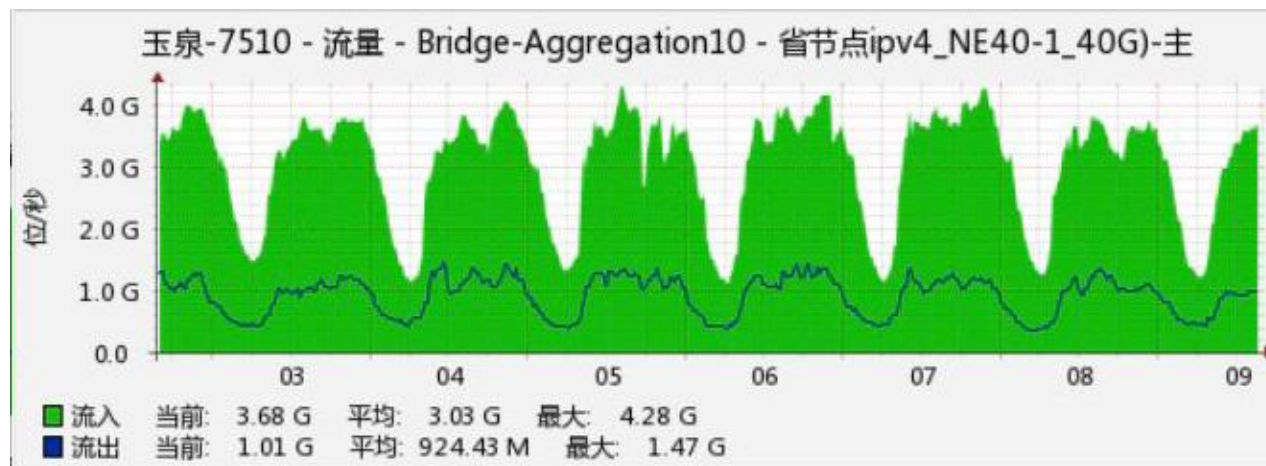
聚合

运营商传输线路（带保护）

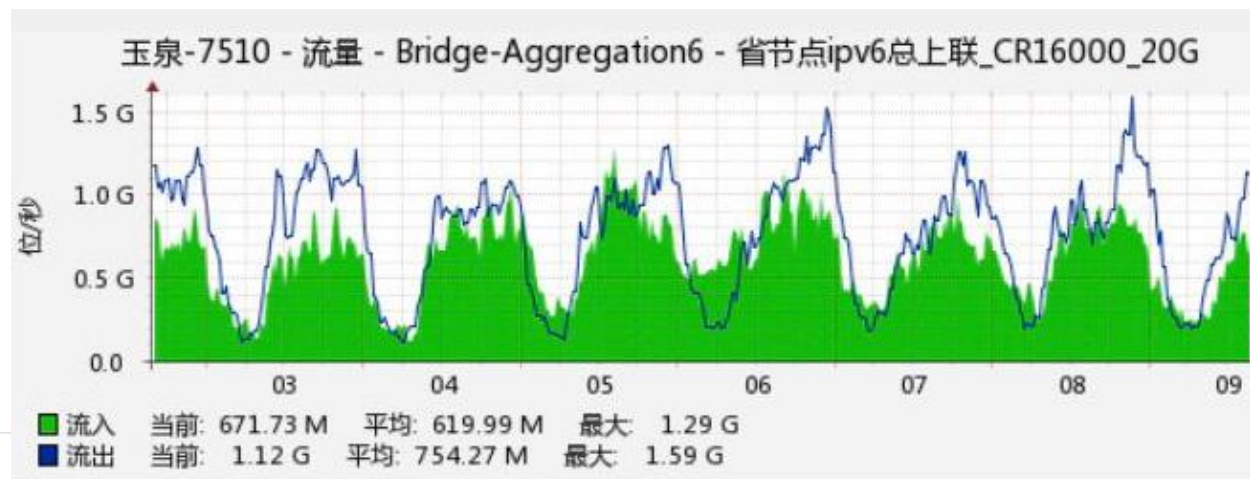


浙江省主节点总流量情况

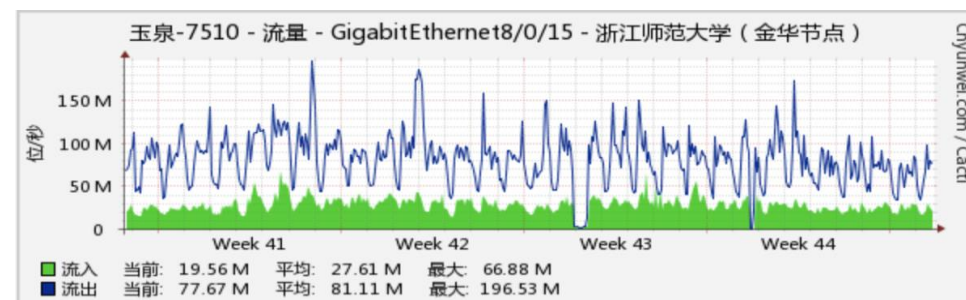
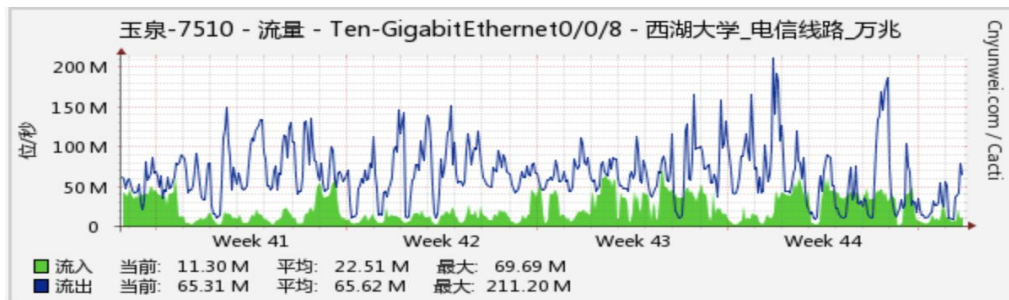
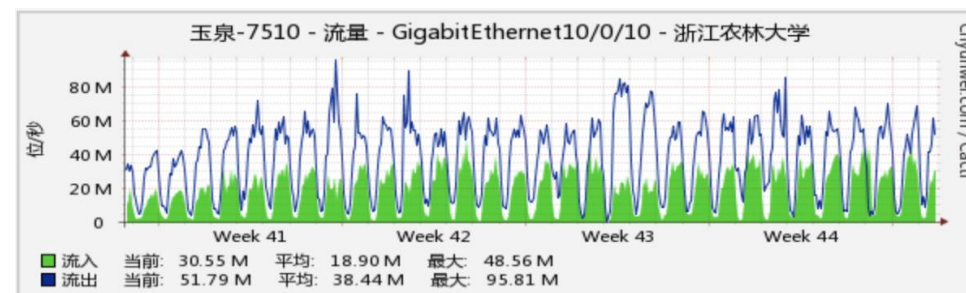
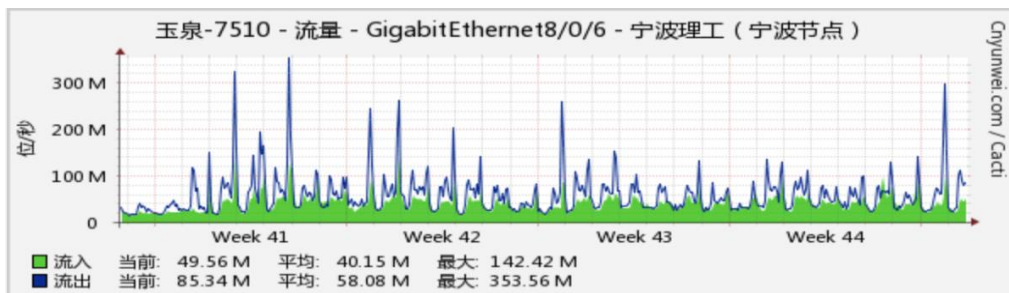
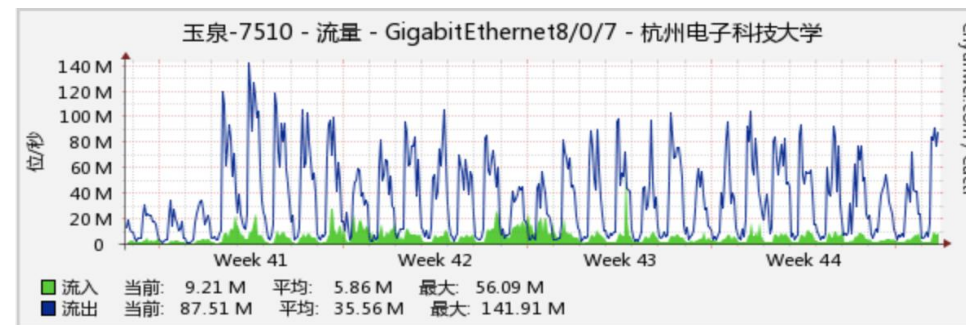
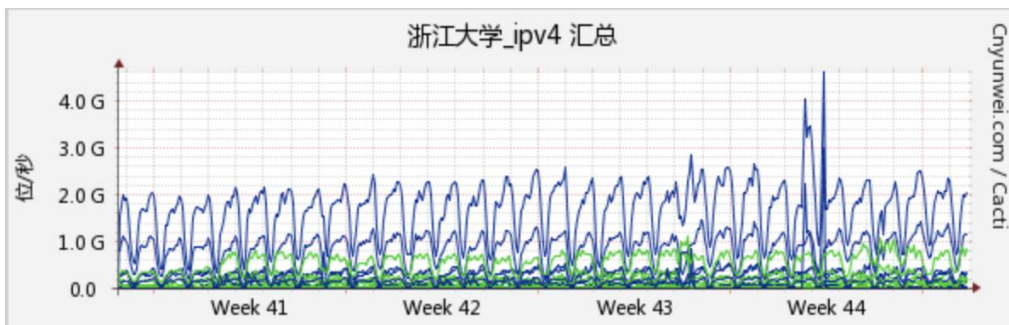
省节点IPv4总流量（近期峰值约4.3G）



省节点IPv6总流量（近期峰值约1.6G）



浙江省部分高校流量情况

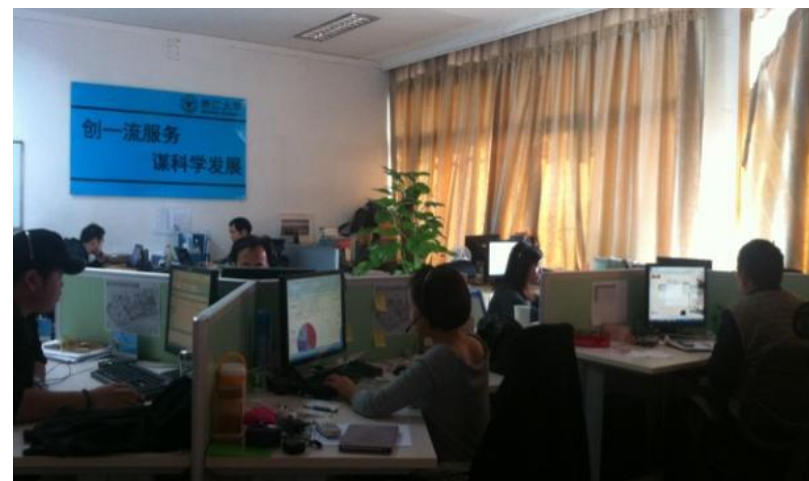


- 健全运维制度

- 7*24小时值班制度
- 开通主节点流量监测运行系统
- 建立故障及时响应处理机制

- 完善节点建设与管理

- 完成主机房UPS电源及线路改造
- 逐步清理收发器、不合规接线板等隐患故障点
- 定期巡检各级各类设备运行情况



/02

网络管理平台

网络管理平台的建设和应用

浙江大学校园网特点突出



- ◆ 如何有效的监控网络运行状态
- ◆ 如何有效的评估网络服务质量
- ◆ 如何有效的感知网络用户体验
- ◆ 如何有效的提升用户获得感

网络管理平台的建设和应用

网络管理平台建设支撑校网运维

浙江大学网络管理与性能监测系统

监控大屏

终端拨测

网络资源监测

硬件探针

软件探针

ICMP协议重构

多线程/高并发

状态监控

远程管理

websocket

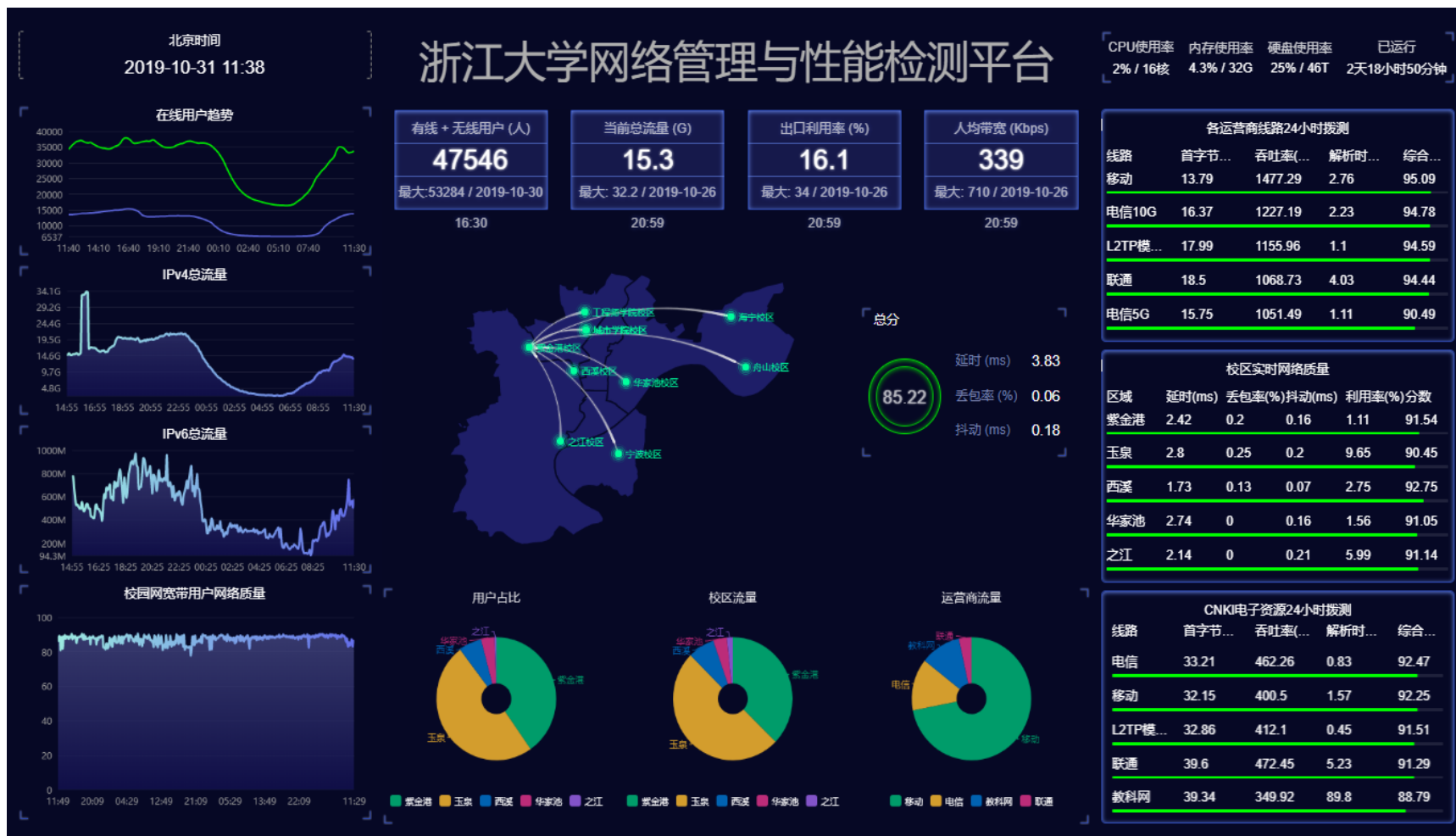
实时回传

网络管理平台的建设和应用

监控大屏作为展现校网质量的窗口

外行看得懂，内行看的清

网络运行，全局展现
关键数据，重点展现
网络变化，图形展现



网络管理平台的建设和应用

分钟级端口监控保障全网有序运行

端口级的网络监控

对全网30+台主要设备，
2w+端口实现分钟级监控，
确保全网稳定运行。被监控
设备类型涵盖交换机、路由
器、防火墙等，监控项目包
括端口状态、CPU利用率、
内存使用率、流量趋势图等

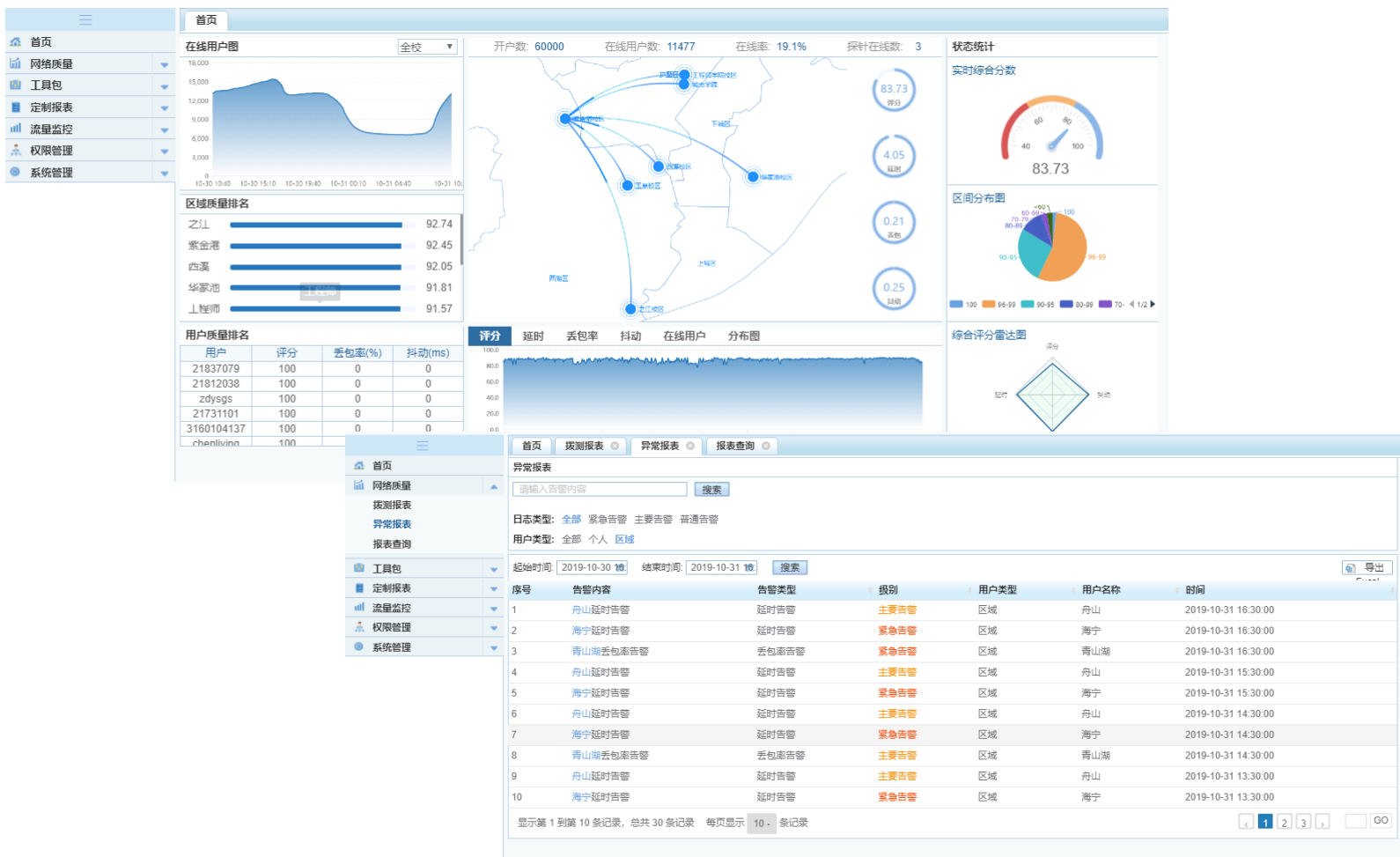


网络管理平台的建设和应用

终端拨测系统真实反映用户网络质量

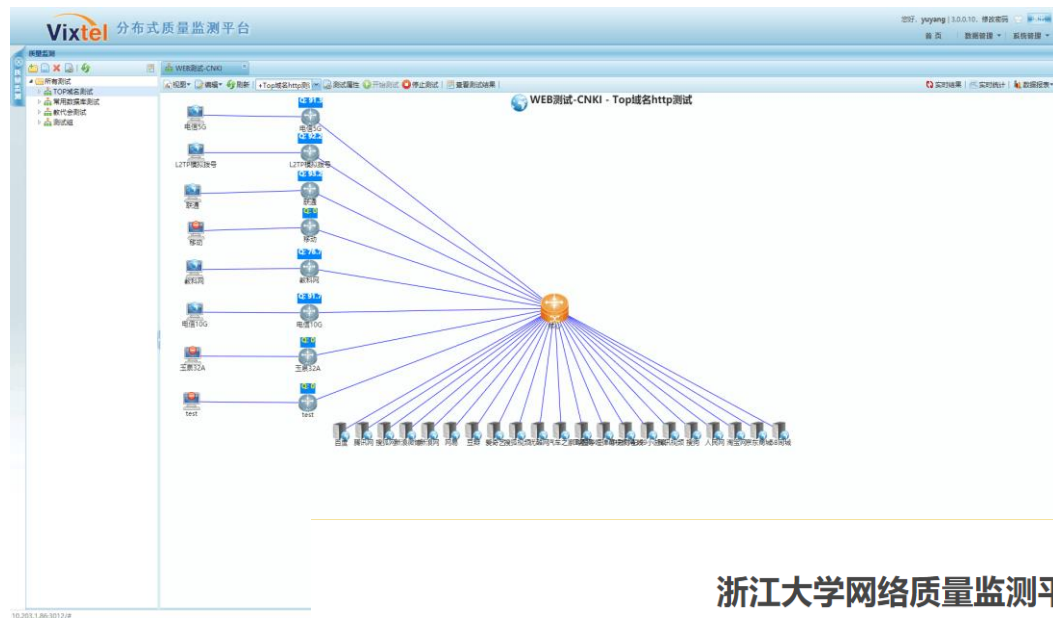
拨测反应真实的网络质量

通过到用户终端的拨测动作，真实反应用户网络使用情况。通过个体的拨测结果聚合，展示各校区的网络质量，对异常情况做到告警提示，实时洞察网络问题。



网络资源实时监控，保证用户使用感知

实时监控网络资源的运行质量，监测的业务应用包括网页访问、视频、下载、游戏等。对有问题的资源第一时间发现，并动态调整路由，保证用户的业务使用体验。



www.baidu.com

查询

序号	线路	IP	评分	DNS解析时间	HTTP连接时间	HTTP传输时间	结束时间	吞吐量(kb/s)	HTTP状态码
1	电信	180.101.49.11	98.80	3.76	41.77	76.22	128.53	1773.77	200
2	移动	183.232.231.174	98.20	5.85	68.34	130.49	216.40	1478.59	200
3	L2TP模拟拨号	180.101.49.12	98.50	1.73	46.93	91.99	159.01	1297.08	200
4	教育网	182.61.200.6	97.00	58.73	122.60	195.72	296.34	1278.65	200
5	联通	112.80.248.75	94.80	4.41	27.47	64.31	137.55	908.46	200



07

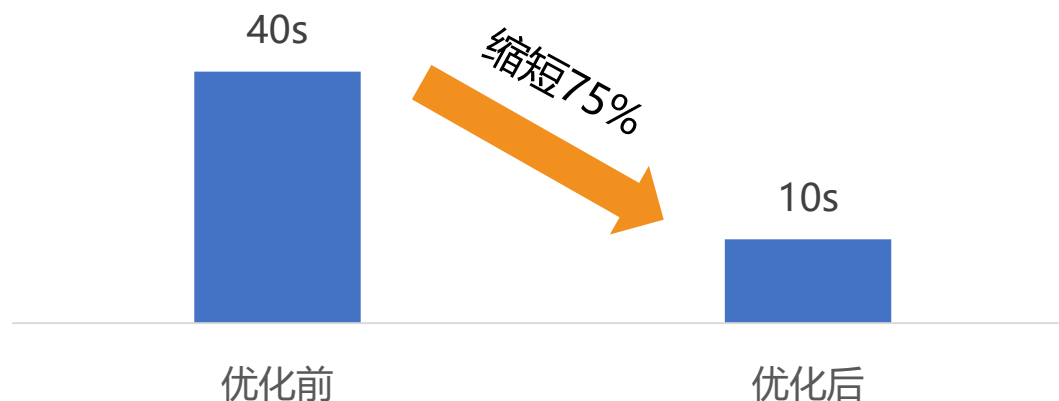
网络管理平台的建设和应用 以数据为依据优化师生用网体验

18个资源7*24监控

最多缩短75%访问用时

90%以上网站打开时间少于10s

Nature下载时间



浙江大学
ZHEJIANG UNIVERSITY

2019/7/9 13:03

/03

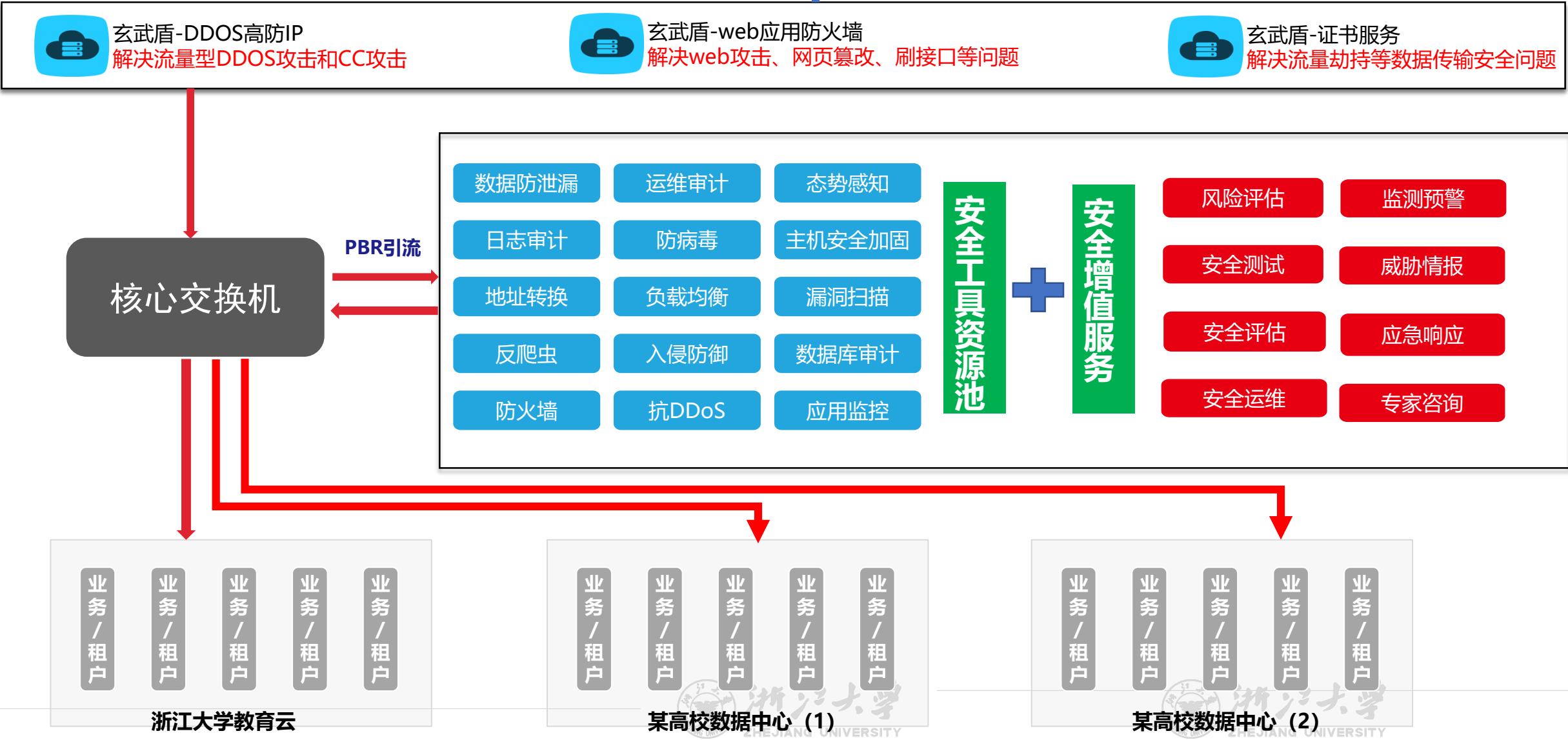
网络安全管理

浙江大学网络安全大会

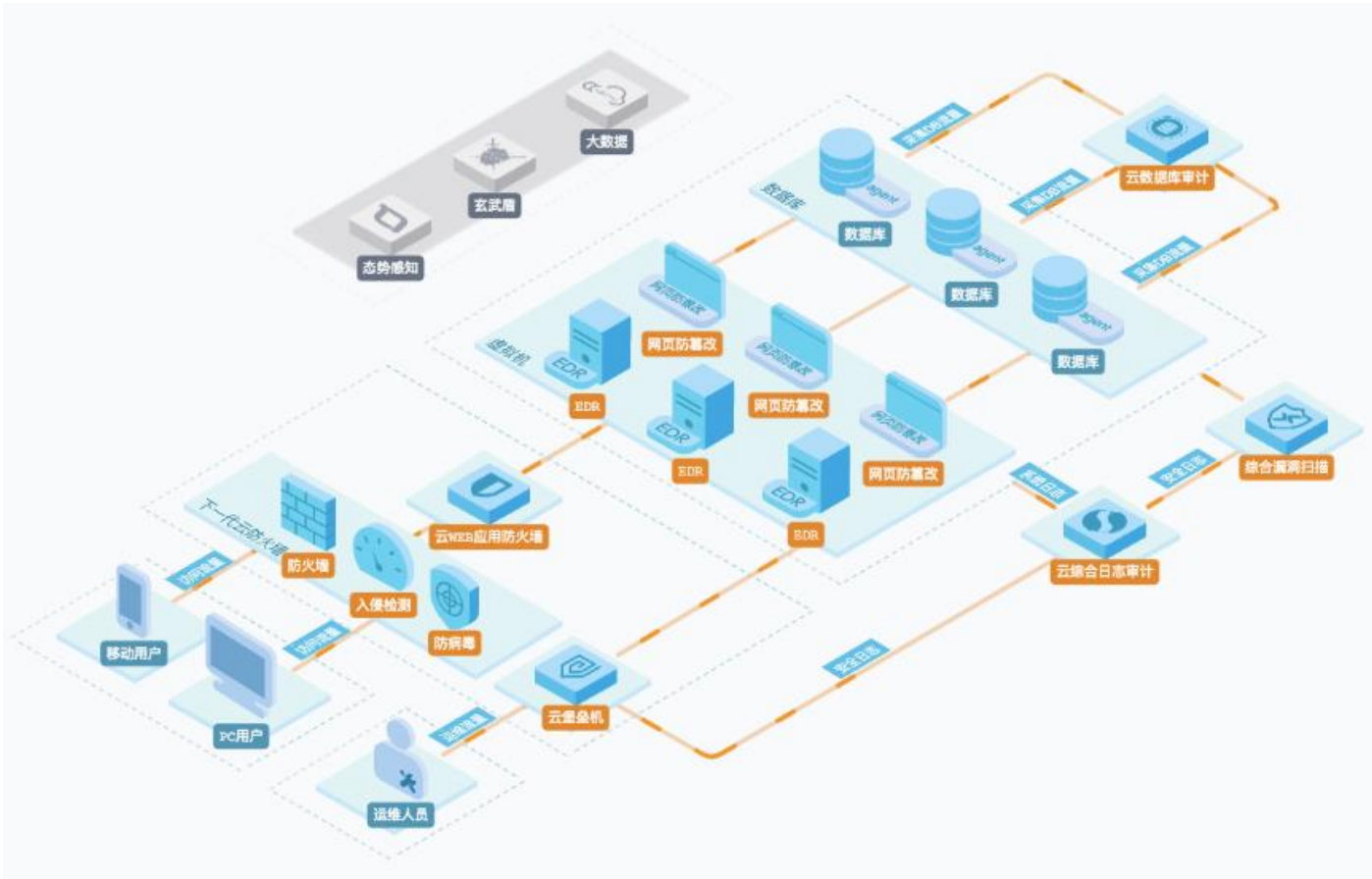
2019年9月16日上午，浙江大学网络安全大会在紫金港校区召开。校党委副书记郑强、校职能部门负责人、各院系部处安全负责人和系统安全全员参加会议。

信息技术中心主任陈文智介绍了我校网络安全现状，并提出要**加快构建关键信息安全保障体系，强化全天候、全方位感知网络安全态势能力，加强学校各方网络安全防御能力和威慑能力，提升我校网络安全整体建设。**





构建云安全资源池，实现云安全能力



下一代云防火墙

- 网络防火墙
- 网络入侵防御
- 网络防病毒

云WEB应用防火墙

- 防御网站威胁、CC攻击
- 业务访问控制
- 网站访问加速

主机安全(EDR)

- 东西向防护
- 主机防病毒

网页防篡改

- 网站文件保护
- 网站目录保护

综合日志审计

- 日志采集归一化处理
- 关联分析、数据挖掘

云运维审计与风险控制系统

- 为用户提供运维审计能力

综合漏洞扫描

- 网站、主机、数据库扫描
- 分析报告
- 提供修复建议

数据库审计

- DB行为监控、操作审计
- 数据分析告警

态势感知

- 提供整个平台的态势感
- 通报预警

大数据

- 大数据安全分析
- 可视化数据展示
- 联动告警

SAAS化WEB防御

- WEB防御监测
- WEB攻击态势感知

网络安全 管理平台

nsm.zju.edu.cn

命名：
浙江大学网络安全管理平台
网络监管与通报平台
网络安全监测平台
事件通报平台
先知

域名：
nsm.zju.edu.cn
jianguan.zju.edu.cn
aqtb.zju.edu.cn
xtzh.zju.edu.cn
xxaq.zju.edu.cn



模块构成



资产管理



安全通报



安全预警



态势分析



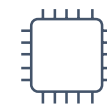
安全监测



威胁情报



应急处置



安全管理

资产管理

资产概览清单

浙江大学网络安全管理平台

资产首页 机构管理 资产审核 资产管理 资产仓库 云服务中心 资产检测 资产发现 指纹管理

资产管理 / 首页

系统资产分析

1300

系统总数



域名资产分析

1083

域名总数



IP资产分析

833

IP总数



单位数量

925



安全人员数量

664



资产新增走势



细分系统分类



统一入口通报威胁

威胁导入

点我下载模板文件

上传文件:

选择

请上传 .zip 文件

关闭

确定

系统管理

漏洞管理

威胁检测

资产治理

态势感知

通报管理

公告管理

系统设置

用户管理

日志管理

帮助文档

漏洞标题

事件类型

涉及url

详细分类

发现时间

漏洞来源

网站所属单位

Poc

来源url

修复建议

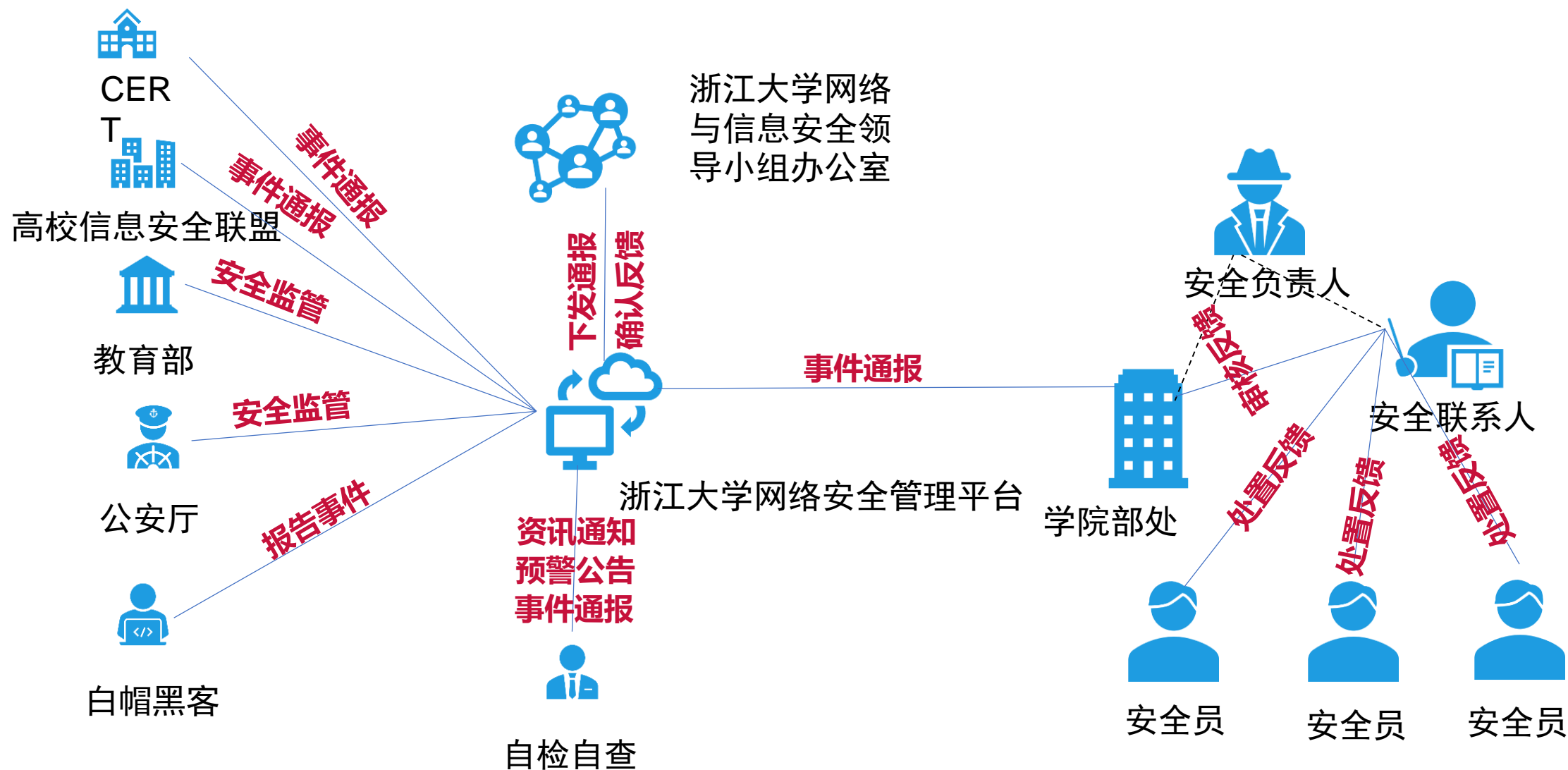
漏洞描述

事件附件

事

~	漏洞	http://xxx/in	任意文件上	2018-08-0	安恒	XXX	博彩	http://xxx/in	修复建议	xx	1.docx	1
---	----	---	-------	-----------	----	-----	----	---	------	----	--------	---

分级处置安全事件



基于地理位置的态势揭示



依托平台形成三个机制

谁主管谁负责、谁运维谁负责、谁使用谁负责

风险报告机制

情报共享机制

研判处置机制

摸清家底

梳理资产1300条；
安全人员664人

认清风险

在应急演练中，平台执行监测任务2项，对210个站点进行漏洞和弱点监测，共发现5080项威胁。其中需紧急处理的漏洞119个。

找出漏洞

通过定期进行漏洞扫描发现内部风险。找出高危漏洞和失陷站点

通报结果

将监测到的安全风险和安全事件进行人工核实后向涉事单位进行通报，实现**风险可管**。

跟踪整改

跟踪涉事单位处置事件的进度和效果，为安全管理考核提供客观数据支撑

/04

规划与建设

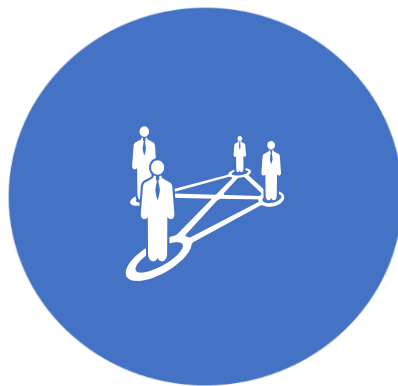
校园无线网络建设背景

无线网应用探索



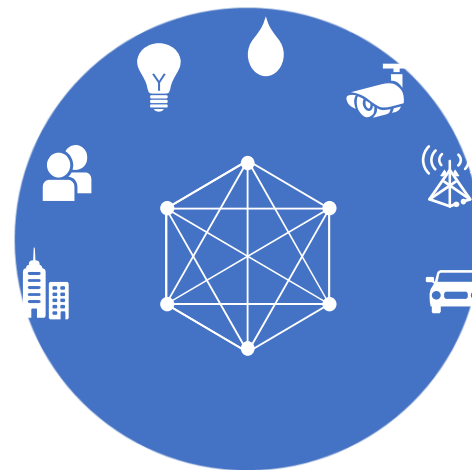
采用802.11g无线AP覆盖部分教学办公区域。

无线网覆盖需求



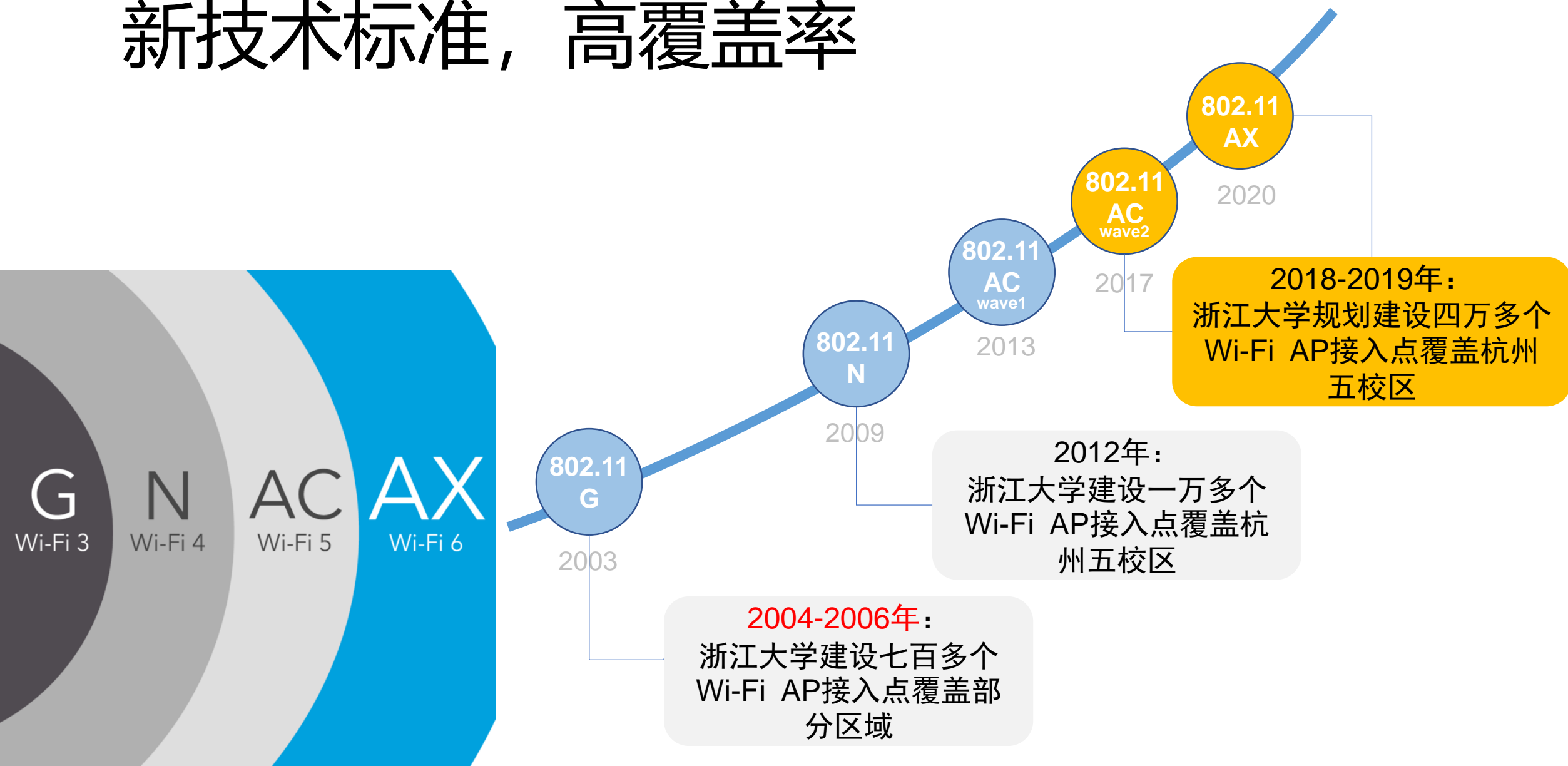
采用近万台802.11n无线AP的校园无线网络，基本实现教学区、宿舍区及室外区域全覆盖。

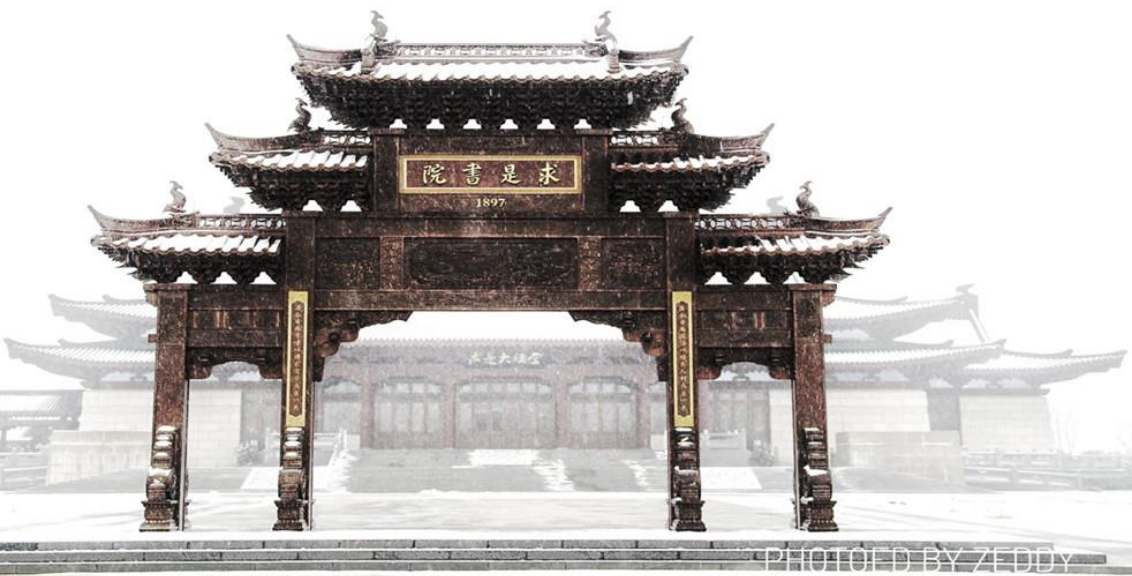
全业务的全联接高速接入



采用802.11ac无线AP完成紫金港、玉泉、西溪、华家池、之江五个校区无线网络全覆盖，全网支持IPv4/IPv6双栈。

新一轮无线网络建设规划： 新技术标准，高覆盖率





谢谢



浙江大学 信息技术中心
INFORMATION TECHNOLOGY CENTER
ZHEJIANG UNIVERSITY