中国科大IPv6应用实践

张焕杰　中国科学技术大学网络信息中心副主任

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
（原中国互联网安全大会）

目录

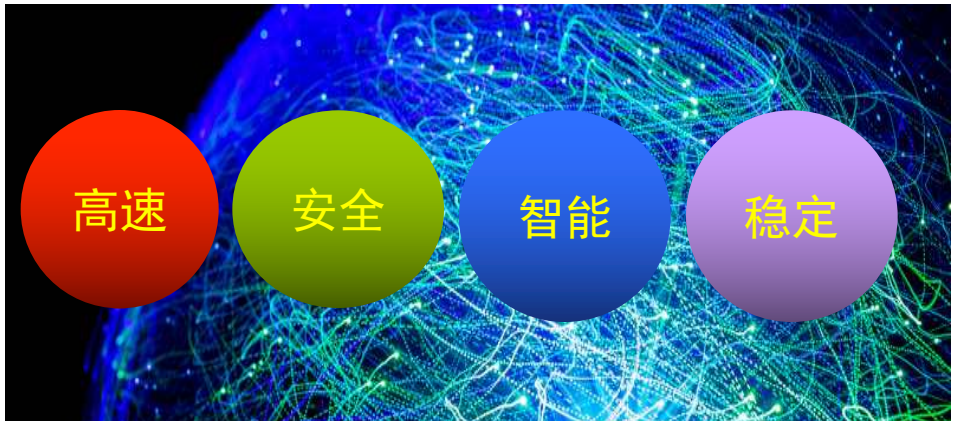
1. 中国科大校园网络简介

- 网络信息中心定位
- 校园网络拓扑
- 校园网络特点

一流的基础设施　支撑一流大学建设

直接服务科学研究过程

文献访问　同行交流　科研协作　应用保障　超算服务



20余年建设校园网络
覆盖校园各个角落

10余年建设超算设施
服务重点科研方向

加大平台建设，增强服务能力

校园网络

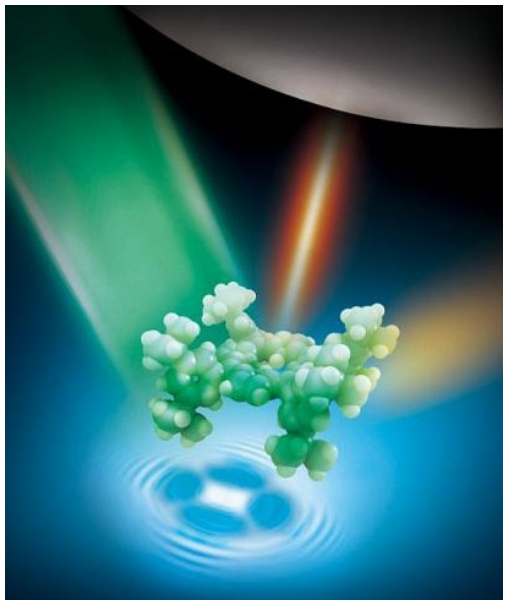
- 承载上网流量、一卡通、视频监控、能源监控等10余套业务
- 7X24保障全校师生正常使用，保障谷歌学术一直可用
- 大陆高校第一家全面开通eduroam学术无线网络漫游服务
- 提供学术带宽，近代物理系与CERN的带宽使用在国内前列
- 参与北京、上海、苏州校区以及先研院的网络规划设计和对接

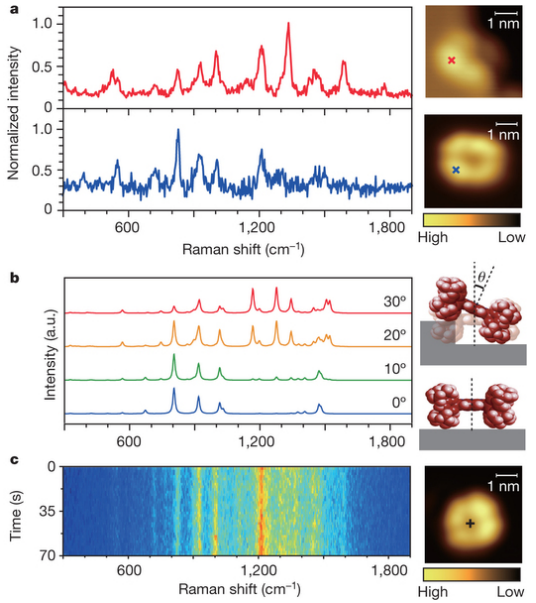
安徽省教育和科研计算机网

- 覆盖16个城市，连接教育厅、考试院和省内近80所高校
- 保障历年高招录取、视频会议等关键应用

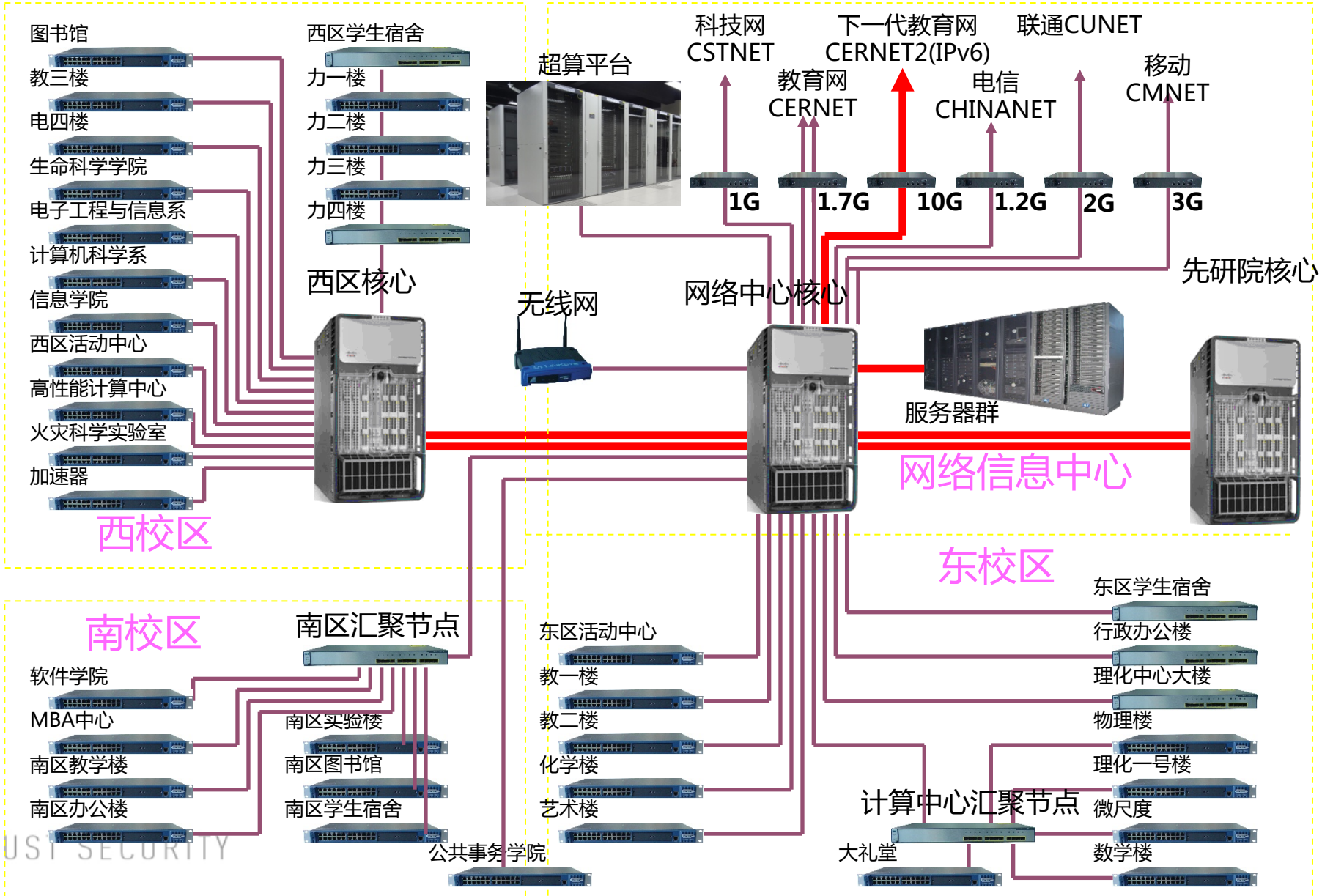
超算中心

- “研究组—校级共享—国家级”三级超算服务模式
- 支持的高水平科研成果不断涌现，发表在nature等一流期刊
- 全校约10%的高水平论文使用超算平台





校园网络拓扑示意图



千兆到桌面

网络资源丰富

用户自主性高

IPv6/v4全支持

ZERO TRUST SECURITY

中国科大校园网特点

充足的网络资源

- 1个自治域号 ASN 45081
- 2B IPv4地址，其中1B+32C直接从CNNIC申请，目前使用了约40%
- /32 IPv6地址

多样的网络出口和丰富的可用带宽

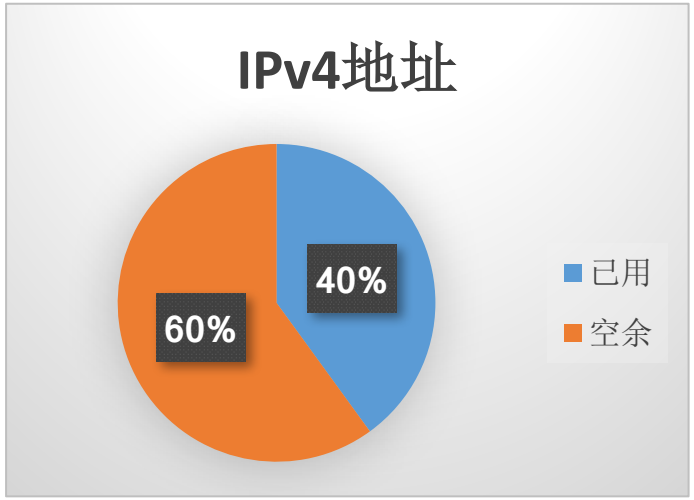
- 2个学术网络出口：中国教育和科研计算机网、中国科技网
- 3个商业网络出口：移动、联通、电信
- 实际使用带宽约13G（2万用户）

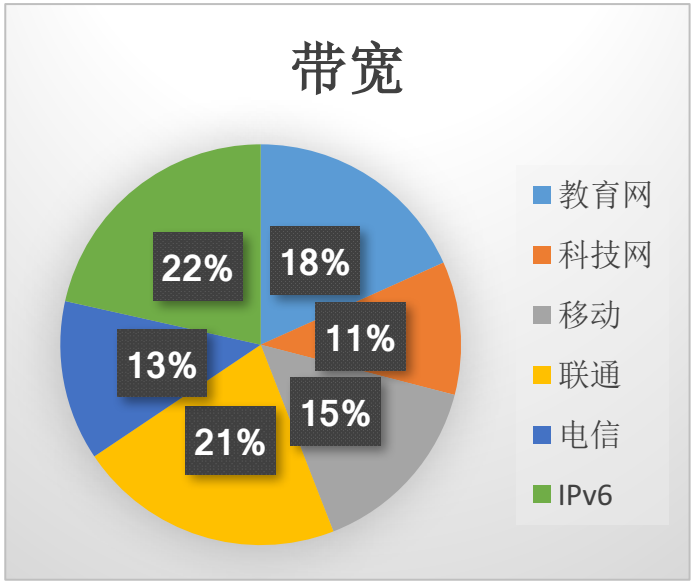
IP协议全支持

- 2005年5月起全校（含OpenVPN用户）网络支持IPv4+IPv6双栈，稳定运行13年
- 目前超过1/2的用户使用IPv6

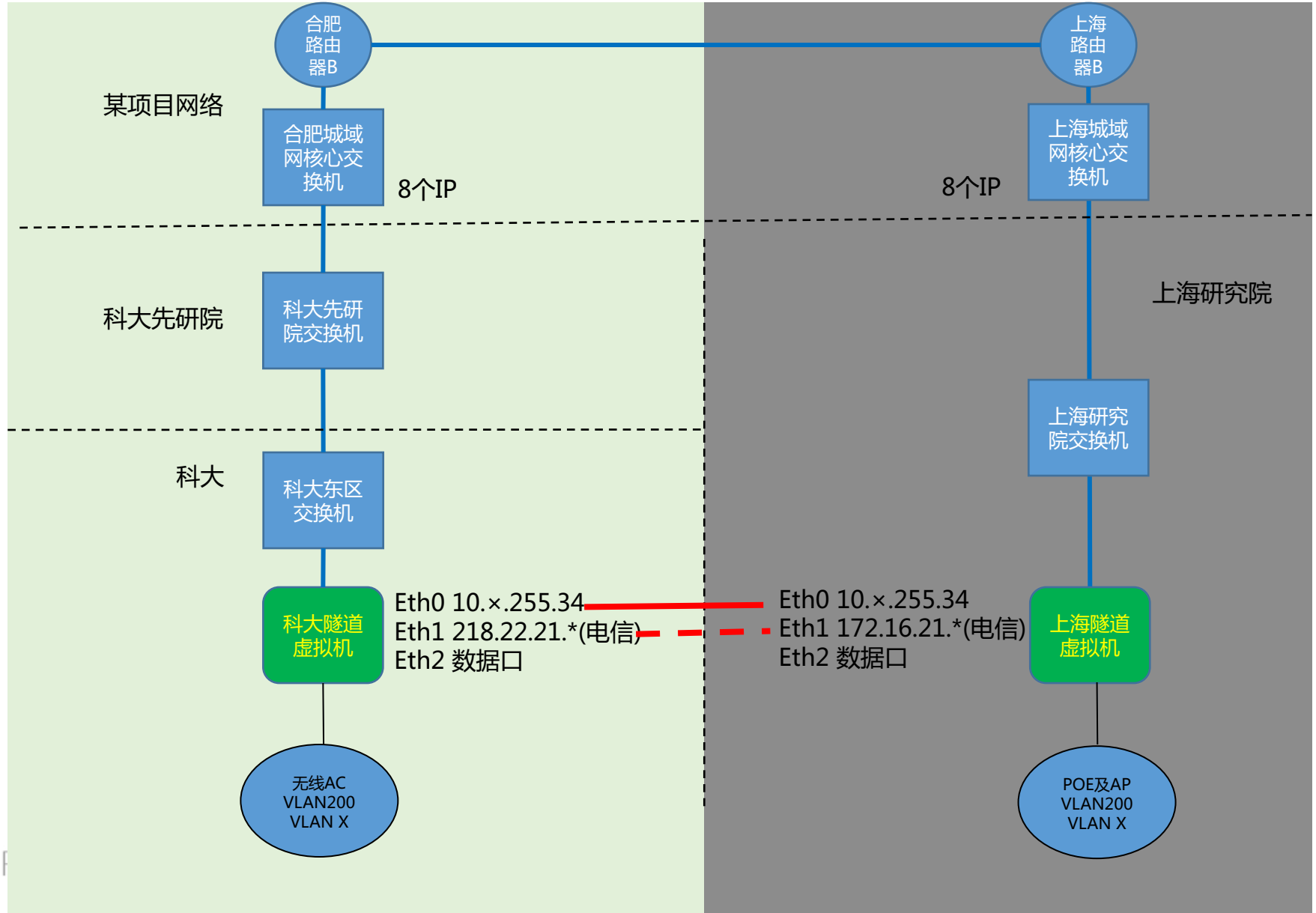
2层为主的校园网

- 自2000年从FDDI改造为千兆以太网后，2层VLAN通达所有位置
- 2层VLAN覆盖合肥的校区和上海研究院





上海研究院VLAN透传

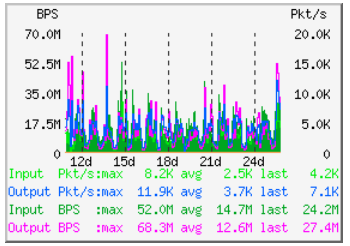


UDP透传以太网包
1G带宽为主线路
电信公网为备用线路
主用线路故障时,3秒钟切换

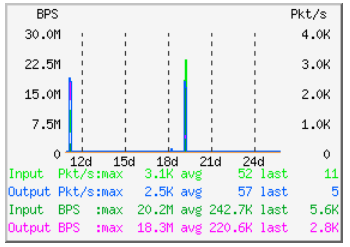
开通的业务：

1. 无线上网，包含eduroam，跟科大本部完全相同
2. 一卡通服务，跟科大本部采用无线连接
3. 上海研究院有线网络用户访问科大本部

主



备



用户自主选择出口路由，随时可以更改

网络通 ×

wlt.ustc.edu.cn/cgi-bin/ip

刷新显示　校内测速　常用设置　退出登录

用户james拥有的权限

序号	权限	状态	到期日	其他
1	VPN接入权限	开通		
2	完全访问权限	开通		最大连接数10

用户9种出口组合
VIP用户+4种

当前IP地址202.38.84.2状态:
出口: 1教育网出口
权限: 国际

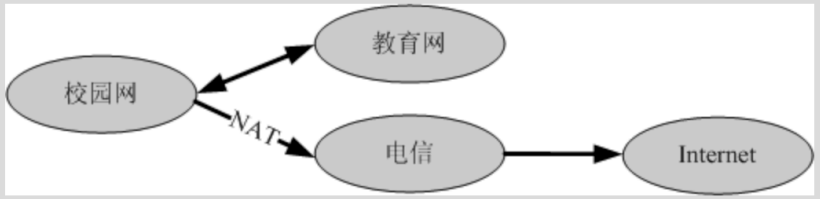
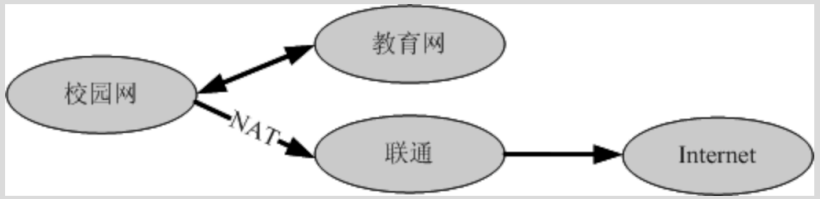
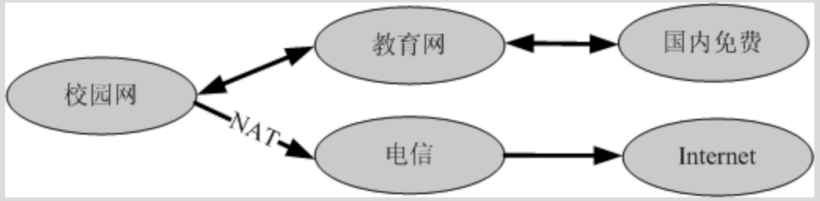
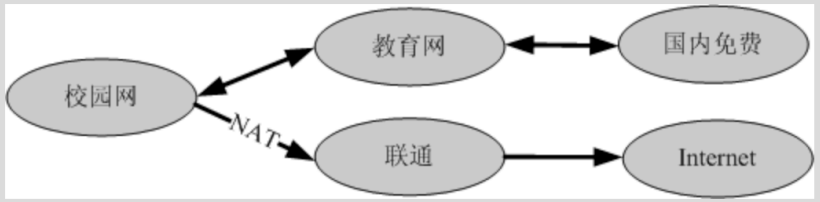
出口选择	使用时限
○ 1教育网出口(国际,仅用教育网访问,适合看文献)	
○ 2电信网出口(国际,到教育网走教育网)	
○ 3联通网出口(国际,到教育网走教育网)	
○ 4电信网出口2(国际,到教育网免费地址走教育网)	
○ 5联通网出口2(国际,到教育网免费地址走教育网)	
○ 6电信网出口3(国际,默认电信,其他分流)	
○ 7联通网出口3(国际,默认联通,其他分流)	
○ 8教育网出口2(国际,默认教育网,其他分流)	○ 1小时
	◉ 4小时
○ 9移动网出口(国际,无P2P或带宽限制)	○ 11小时
	○ 14小时
◉ 10科技网科研专线出口(国际,无P2P或带宽限制,科研专线)	○ 永久
○ 11电信网科研专线出口(国际,无P2P或带宽限制,科研专线)	
○ 12移动网科研专线出口(国际,无P2P或带宽限制,科研专线)	
○ 13电信与移动自动选择(国际,无P2P或带宽限制,科研专线)	

如访问文献资源或进行P2P下载，建议使用1或9出口

网络通 × 网络通 ×

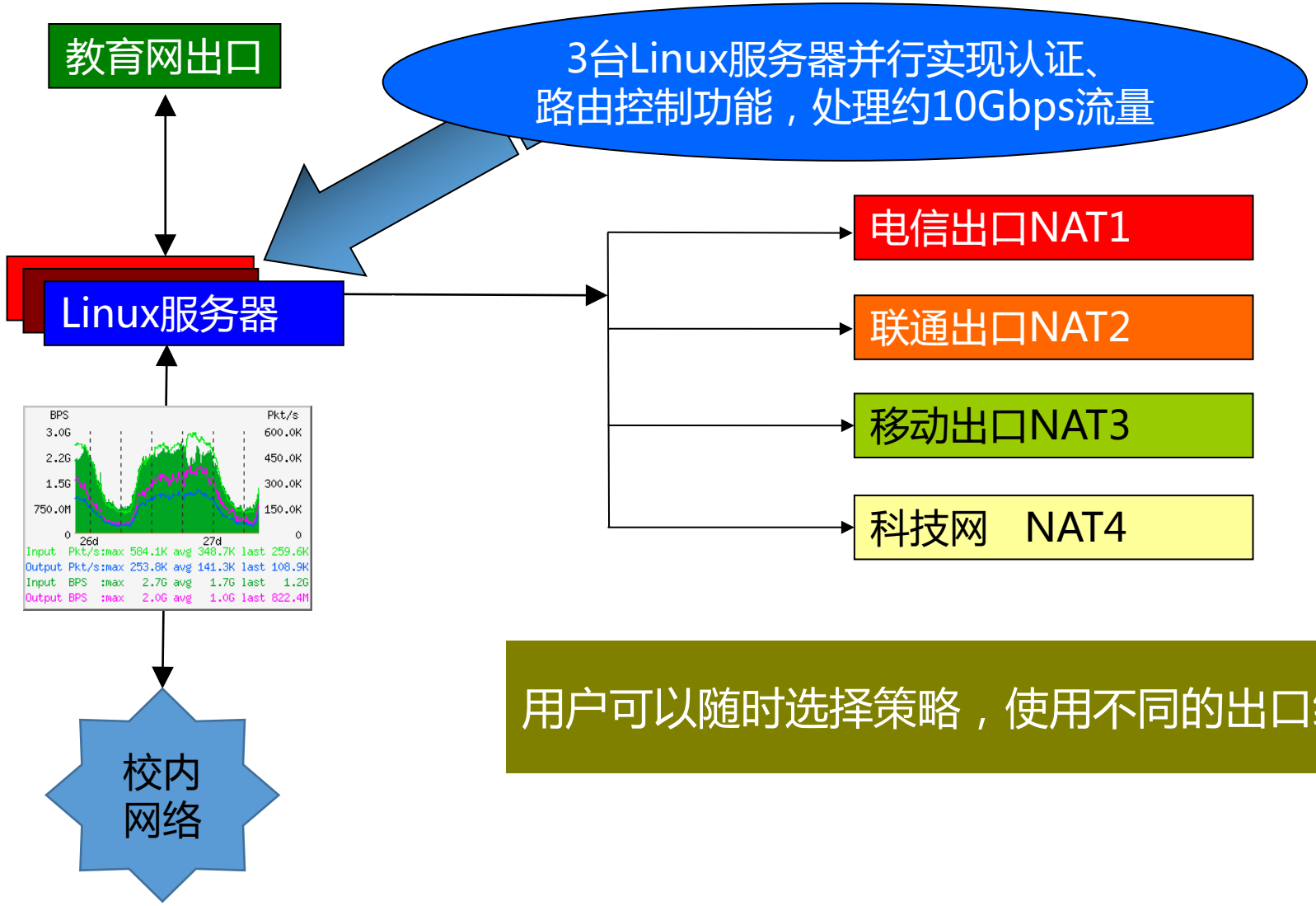
wlt.ustc.edu.cn/link.html

使用完全权限的网络通，可以有9种出口选择方式：

出口选项	数据流示意图	
1. 教育网出口		走教育网，不经过地址转换(NA
2. 电信网出口		到教育网走教育网，其他经过N
3. 联通网出口		到教育网走教育网，其他经过N
4. 电信网出口2		到教育网定义的免费地址走教育
5. 联通网出口2		到教育网定义的免费地址走教育

校园网络出口拓扑图

其中一台Linux机器
连续运行超过11年

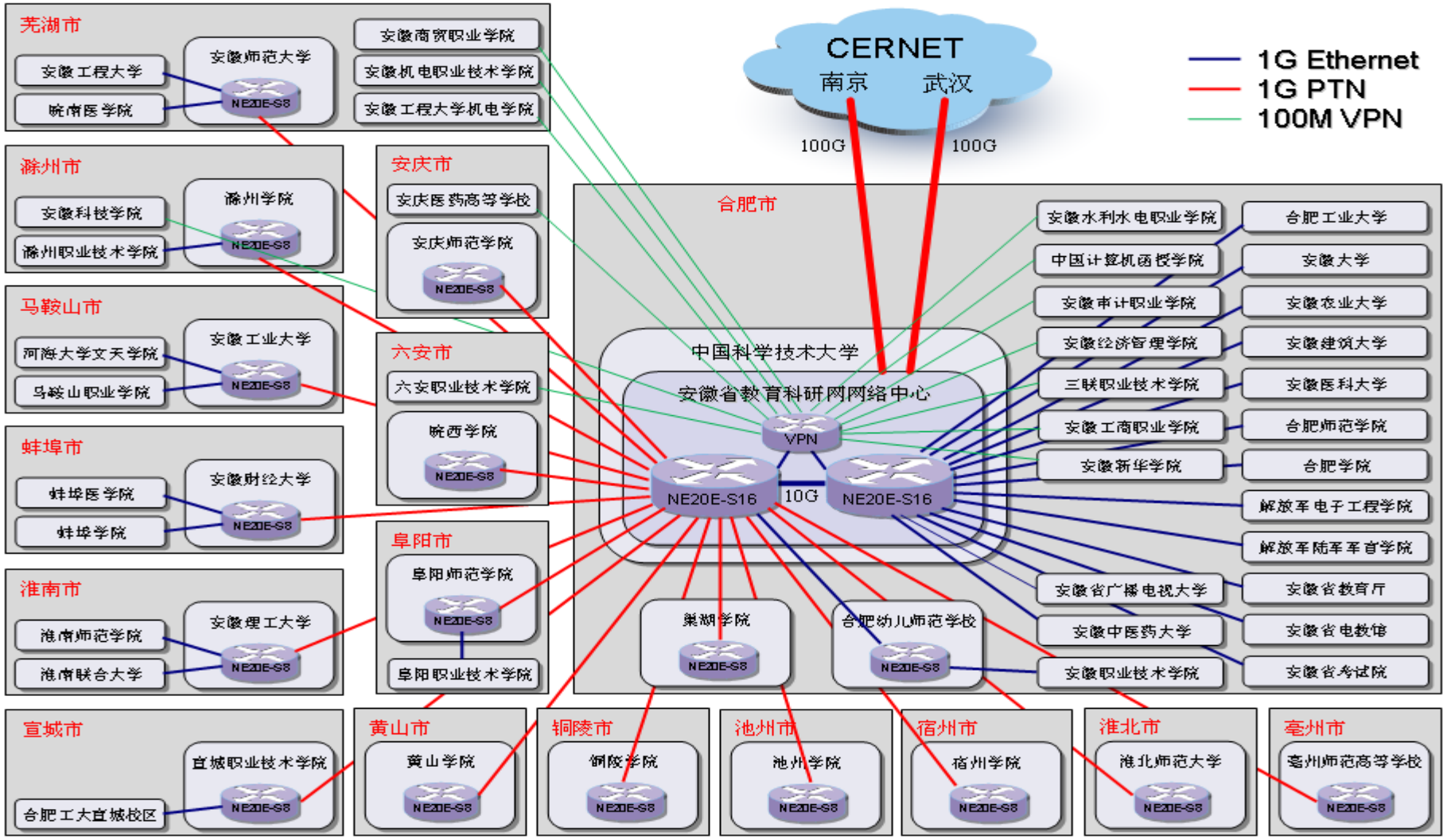


用户可以随时选择策略，使用不同的出口组合

2. 安徽省教育和科研计算机网络简介

- 安徽省教育和科研计算机网络拓扑
- 安徽省教育和科研计算机NOC

安徽省教育和科研计算机网主干



省级教育行业主干网
连接近80所高校

支持IPv4/IPv6协议

安徽省教育和科研计算机网主干

◆线路与协议

合肥部分高校10G+1G线路

省内各城市1G线路+VPN备用线路

部分学校VPN线路接入

支持IPv6/IPv4双栈

◆路由协议

内部主干使用OSPF+OSPFv3协议

BGP承载用户路由

对外：CERNET　静态路由

CERNET2 BGP

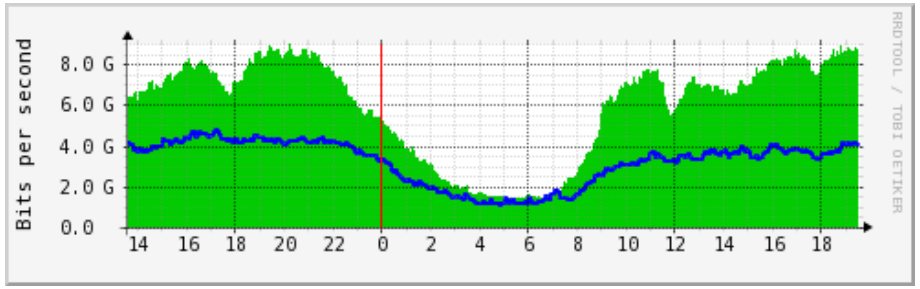
◆冗余性

主干线路1G+VPN备用线路

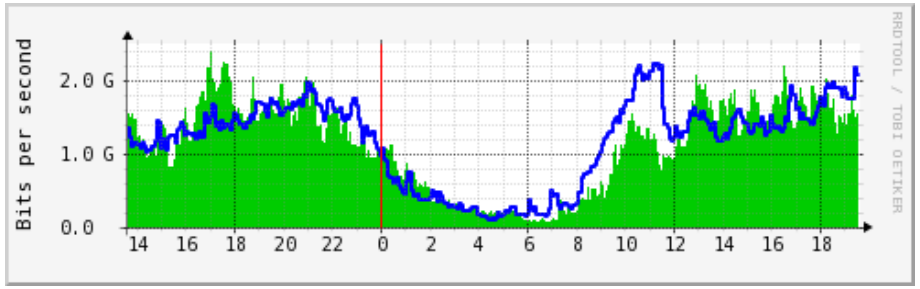
合肥局部光纤环网

部分高校双路由裸光纤，动态路由或port channel备用

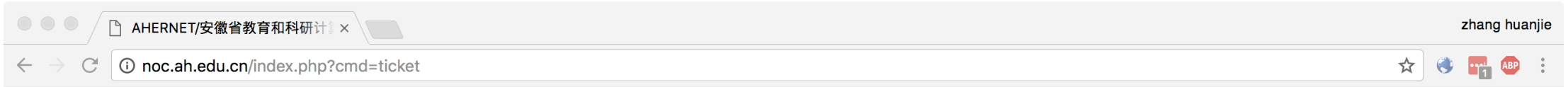
IPv4总流量



IPv6总流量



安徽省教育和科研计算机网NOC

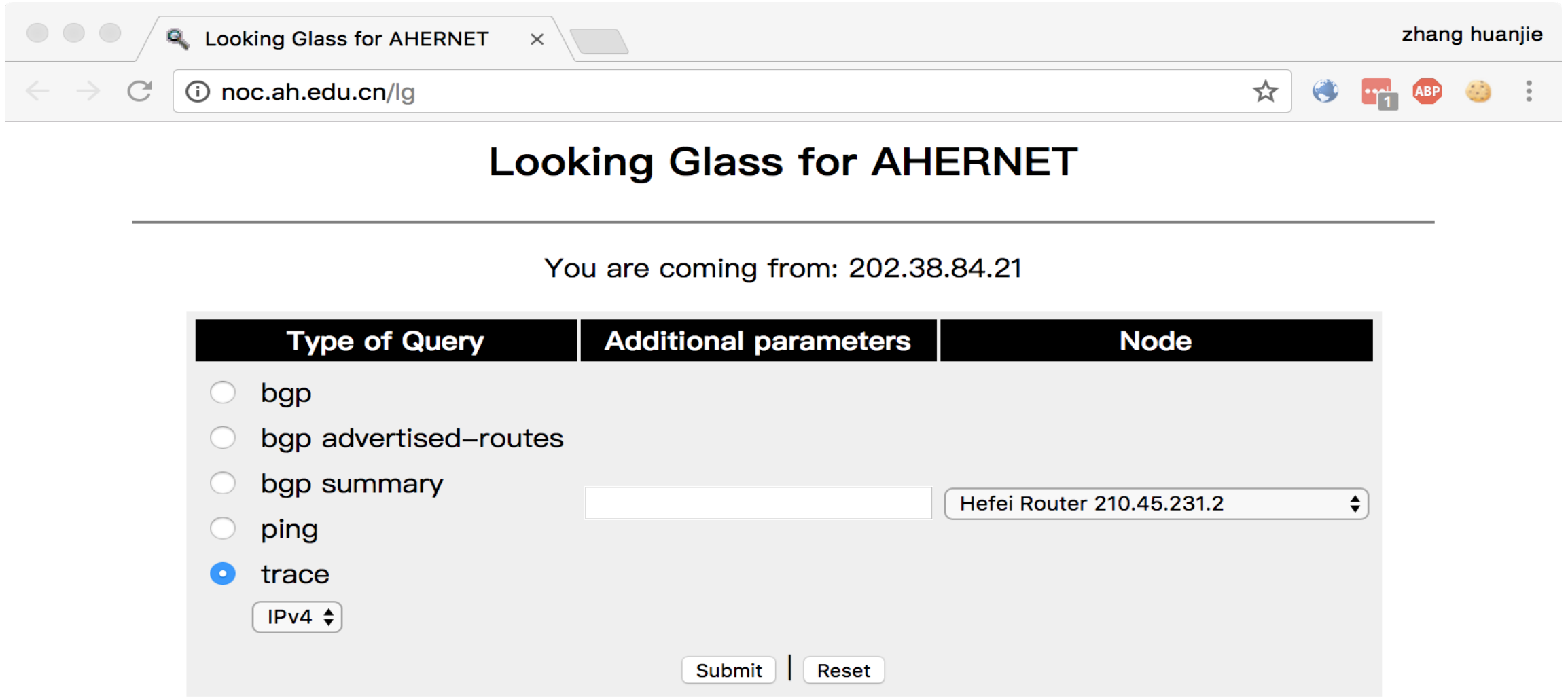


网络状况 事件记录 接入单位 IP地址汇总 详细IP地址 常用信息 MAC查询 Looking Glass 登录 From:202.38.84.142 有任何问题请联系 james@ustc.edu.cn

2013.06.01之前的记录 列出所有记录 2018故障统计

序号	开始时间	结束时间	影响节点	中断时间	事件描述	时间	处理
1	2018-04-18 17:27:29	2018-04-18 18:21:00	2	0.9小时	安徽大学机房停电	2018-04-18 17:27:29	停电
						2018-04-18 18:21:00	恢复
2	2018-04-17 11:08:27	0000-00-00 00:00:00			滁州职业学院改用SFP模块	2018-04-17 11:08:27	改用单芯SFP模块
3	2018-04-08 16:11:42	2018-04-09 11:07:11		18.9小时	马鞍山1G中断	2018-04-08 16:11:42	1G专线中断
						2018-04-09 11:07:11	恢复
4	2018-04-04 10:30:00	2018-04-12 11:00:00		192.5小时	安徽冶金科技职业学院	2018-04-04 10:30:00	GRE VPN调试
						2018-04-12 11:00:00	更换为专线
5	2018-04-04 08:42:01	0000-00-00 00:00:00			CNGI 100G线路启用	2018-04-04 08:42:01	更换到新设备
6	2018-03-28 17:26:58	2018-04-09 16:25:17		287小时	考试院东区-教育厅中断	2018-03-28 17:26:58	教育厅收无光
						2018-04-09 16:25:17	恢复
7	2018-02-23 15:18:03	2018-02-23 17:10:32	3	1.9小时	蚌埠中断	2018-02-23 15:18:03	电力改造停电
						2018-02-23 17:10:32	恢复
8	2018-02-18 12:38:31	2018-02-22 14:36:57		98小时	考试院东区-教育厅中断	2018-02-18 12:38:31	教育厅收光低
						2018-02-22 14:36:57	恢复
9	2018-02-11 18:37:15	2018-02-11 19:20:51		0.7小时	池州中断	2018-02-11 18:37:15	机房更换UPS电池
						2018-02-11 19:20:51	恢复
10	2018-02-11 13:28:53	2018-02-11 14:45:25	3	1.3小时	马鞍山中断	2018-02-11 13:28:53	移动传输设备掉电
						2018-02-11 14:45:25	恢复
						2018-02-11 16:17:09	VPN恢复
11	2018-02-08 09:26:17	2018-02-08 17:13:46		7.8小时	淮南联大中断	2018-02-08 09:26:17	光缆中断
						2018-02-08 17:13:46	恢复
12	2018-02-02 17:00:00	0000-00-00 00:00:00			CNGI路由器上线	2018-02-02 17:00:00	CNGI路由器上线

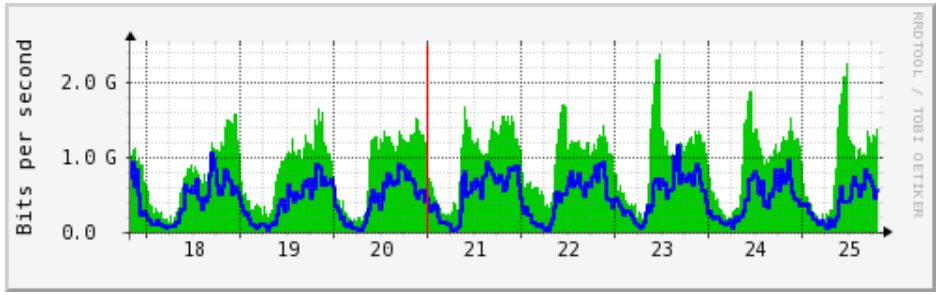
安徽省教育和科研计算机网LOOKING GLASS



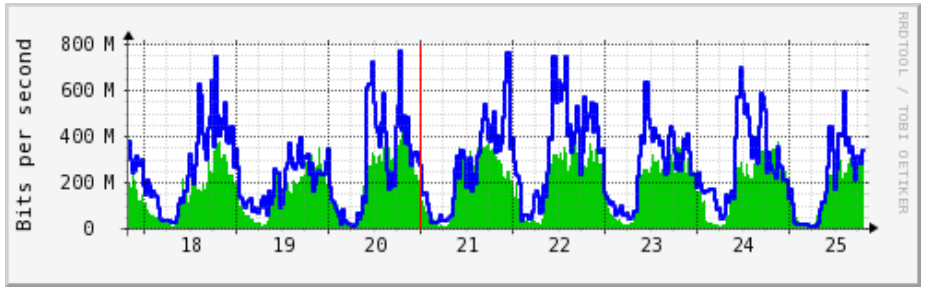
ZER

IPV6流量

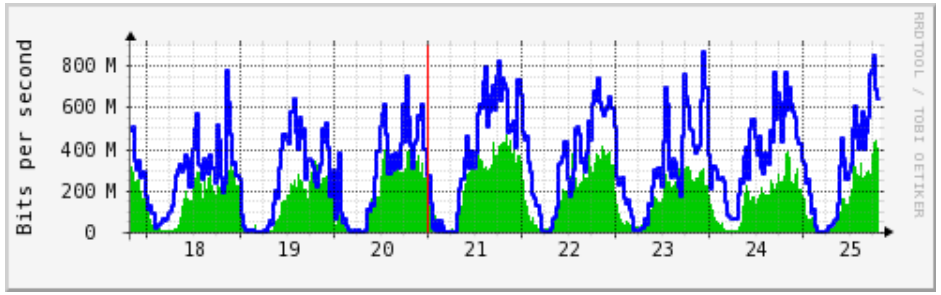
中国科学技术大学



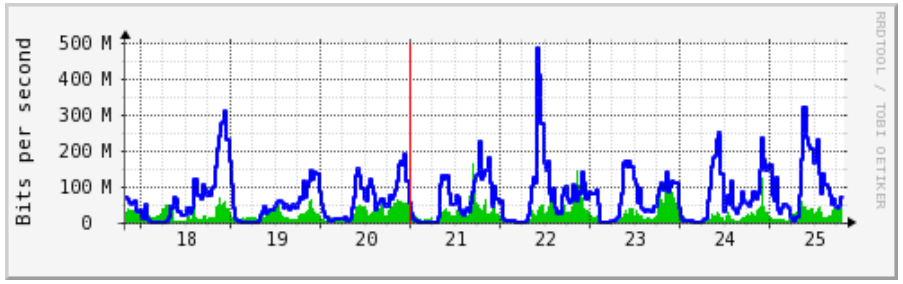
合肥工业大学



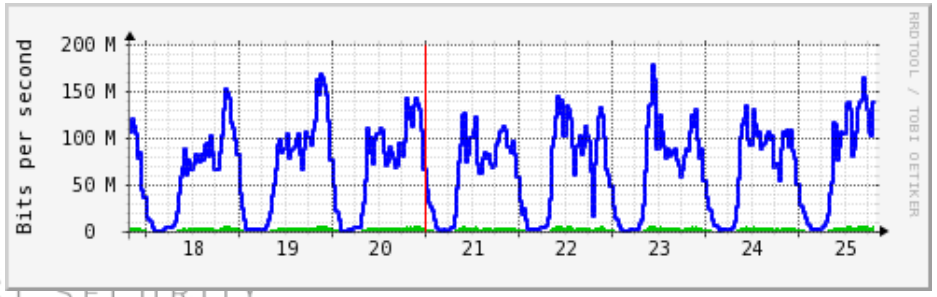
安徽大学



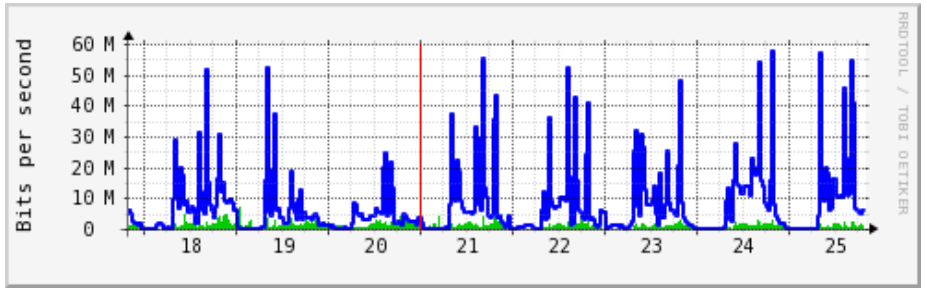
安徽农业大学



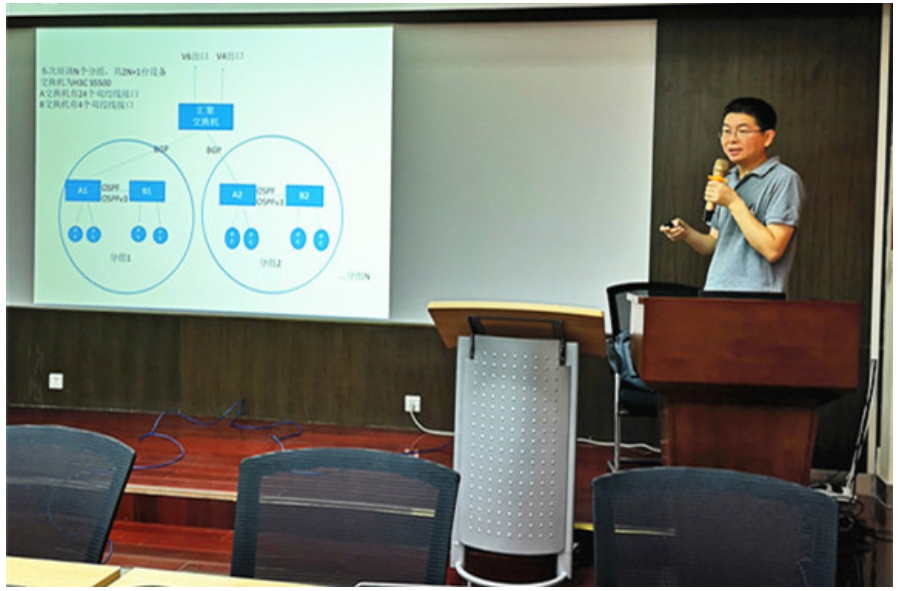
安徽师范大学

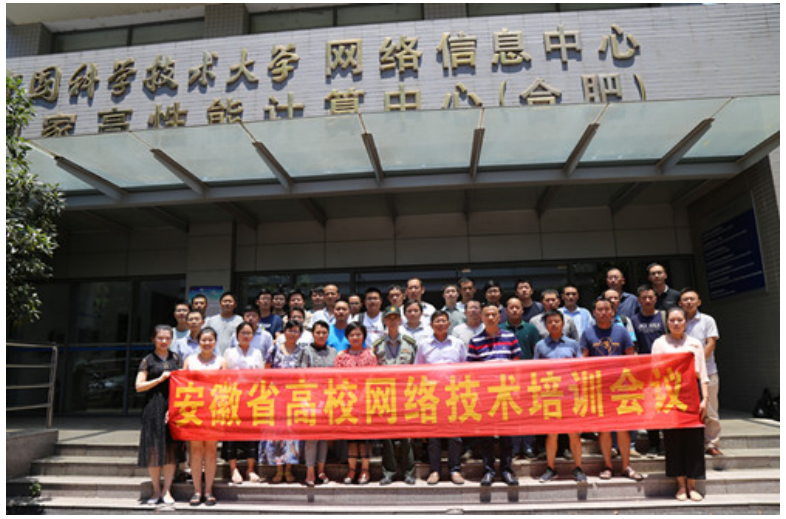


滁州学院



IPV6技术培训





每期40人，分8组

OSPF/OSPFv3/BGP配置　3小时
Nginx/Letsencrypt配置　3小时

3期，112人参加培训

参加培训后， 15所学校开通了IPv6服务

3. 校园网IPV6应用与管理

- IPV6发展历史
- IPV6用户接入
- IPV6服务提供
- IPV6运行监测
- IPV6安全措施

中国科大校园网IPV6历史

1999年

李津生教授承担863课题《中国科大IPv6示范网》

2000年

采用纯IPv6链路和隧道技术相结合的组网技术，建成校内IPv6测试网

2004年

CNGI-CERNET2中国科学技术大学节点建成

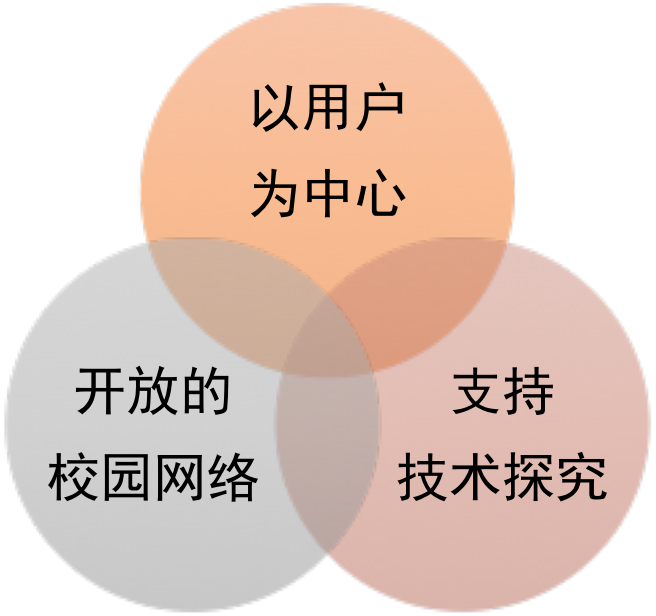
2005年

校园网改造为万兆主干，校内全面支持IPv6，包括OpenVPN的远程用户均支持IPv6

2017年

反向代理支持IPv6，600余个网站正式提供IPv6服务

网络管理理念



接入方式丰富，满足各种用户需要
使用方便快捷，尽量少设置障碍

如支持LUG(学生Linux协会)开展PXE启动、
开源软件镜像等技术探究

https://mirrors.ustc.edu.cn/
Debian、Ubuntu、Fedora、Archlinux、CentOS等多个发行版的官方源
大陆高校访问量最大、收录最全的两个开源软件镜像之一

使用标准协议，只要是TCP/IP系统，都可以接入
只要不违反法律法规、不影响网络运行，都应该支持

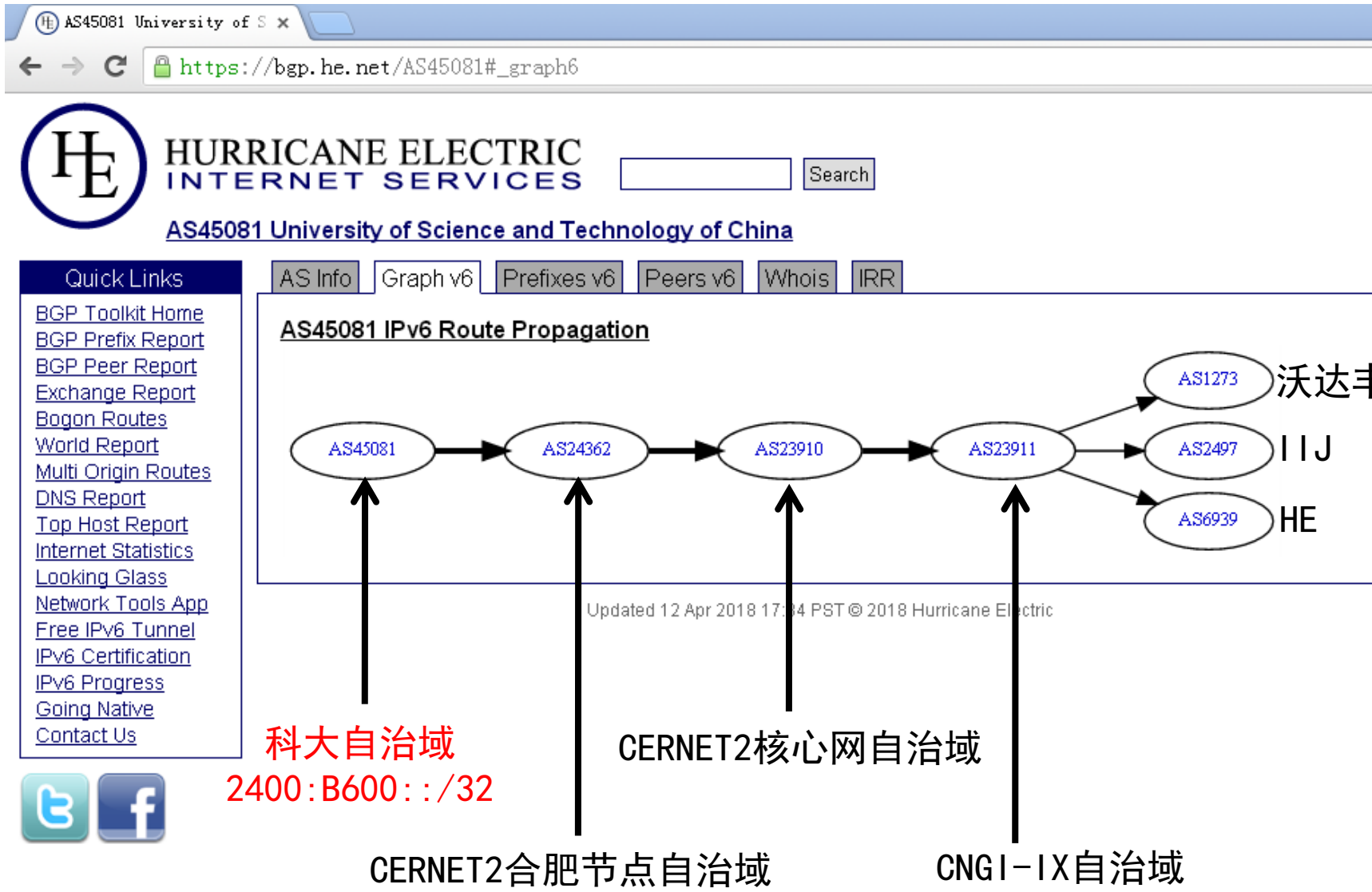
IPV6主干

万兆主干

- 3台三层交换机和1台BRAS处理3层路由
- 其他设备仅作二层交换机使用
- IPv4/IPv6双栈

路由协议

- 4台三层设备之间路由协议为OSPFv3
- BGP协议与CNGI-CERNET2接入设备互通
- 部分静态路由



用户IPV6接入

校内接入无认证

- 校内办公区、宿舍区、无线网络直接接入

无状态地址分配

- 使用无状态方式分配IPv6地址
- 只要安装IPv6协议就能分到地址，最大程度方便用户

校外用户

- OpenVPN，通过电信、联通、移动网络出口提供用户接入

VLAN接口配置

```
interface Vlan167
ip address 202.38.81.254/25
ip verify unicast source reachable-via rx
ipv6 address 2001:da8:d800:81::1/64
ipv6 verify unicast source reachable-via rx
ip dhcp relay address 202.38.64.7
```

BRAS接口配置

```
interface Route-Aggregation1.500
  vlan-type dot1q vid 500 second-dot1q 51 to 900
  dhcp select relay
  ipv6 address 2001:DA8:D800:500::1/64
  ipv6 address auto link-local
  ipv6 nd autoconfig other-flag
  undo ipv6 nd ra halt
  ipv6 nd ra router-lifetime 9000
  ipv6 subscriber l2-connected enable
  ipv6 subscriber initiator ndrs enable
  ipv6 subscriber initiator unclassified-ip enable
  ipv6 subscriber user-detect nd retry 5 interval 60
  ipv6 subscriber unclassified-ip domain ustcipv6
  ipv6 subscriber ndrs domain ustcipv6
```

开发一个简单的radius服务器，
仅仅允许特定的地址段上线

子网用户的IPV6接入

子网很普遍，有接入IPv6需求

- 不少实验室/办公室建立子网，通过地址转换设备连接到校园网
- 可以将IPv6数据包桥接到内网，让内部用户使用IPv6
- 也可以分配独立网段，设置静态路由

子网用户的独立网段IPV6接入

- 给子网分配IPv6 /64前缀，核心交换机设置静态路由

子网管理员在子网的网关设备上设置如下信息

- 内外接口IPv6地址，默认路由
- 设备内部的RA广播
- 启用路由功能

中科大校园网IPV6应用服务

基础IPv6环境

- DNS、OpenVPN

现有应用的IPv6原生支持

- BBS/IPTV/FTP/个人主页/高性能计算等

网站的大规模服务支持

- 使用nginx反向代理服务器，对外统一提供IPv6+SSL支持

互联网根DNS服务器

13个 a.root-servers.net … m.root-servers.net

- http://www.internic.net/domain/named.root
- 每个有IPv4、IPv6地址
- 13个的原因是DNS数据包最大512字节的限制

实际上远远不止13个

- 很多服务器在13个IP地址上提供服务(AnyCast)
- http://root-servers.org/ 公布有官方的，大约几百个
- 真实的服务器数量没有人能准确知道

教育网内的根域名服务器

- 测量到根域名服务器的IPv4地址延迟，可以判断教育网内有12个根域名服务器
- 0ms f j
- 30ms a b c d e g i k l m

30ms以内的延迟，在教育网内

- 300ms h

这个不在教育网内

互联网根DNS服务器

任何人都可以做根域名服务器

- 任何人只要下载 https://www.iana.org/domains/root/files
- 配置好bind，就可以提供根域名服务

要想使用方便，需要劫持相关的路由

- 教育网劫持了12个根域名服务器的IPv4路由
- 我校自己提供根域名服务
- 劫持了13个根域名服务器的IPv6路由和1个IPv4路由

相关说明

- https://github.com/bg6cq/ITTS/blob/master/app/dns/root/README.md

校园网劫持的路由

show ip route

198.97.190.53/32, ubest/mbest: 1/0

*via 202.38.64.12, [20/0], 8w0d, bgp-45081, external, tag 65500

show ipv6 route

2001:500:1::53/128, ubest/mbest: 1/0

*via 2001:da8:d800::12, Vlan640, [20/0], 8w0d, bgp-45081, external, tag 65500

2001:500:2::c/128, ubest/mbest: 1/0

2001:500:12::d0d/128, ubest/mbest: 1/0

2001:500:2d::d/128, ubest/mbest: 1/0

2001:500:2f::f/128, ubest/mbest: 1/0

2001:500:9f::42/128, ubest/mbest: 1/0

2001:500:a8::e/128, ubest/mbest: 1/0

2001:500:200::b/128, ubest/mbest: 1/0

2001:503:c27::2:30/128, ubest/mbest: 1/0

2001:503:ba3e::2:30/128, ubest/mbest: 1/0

2001:7fd::1/128, ubest/mbest: 1/0

2001:7fe::53/128, ubest/mbest: 1/0

2001:dc3::35/128, ubest/mbest: 1/0

知名学校主网站特性对比

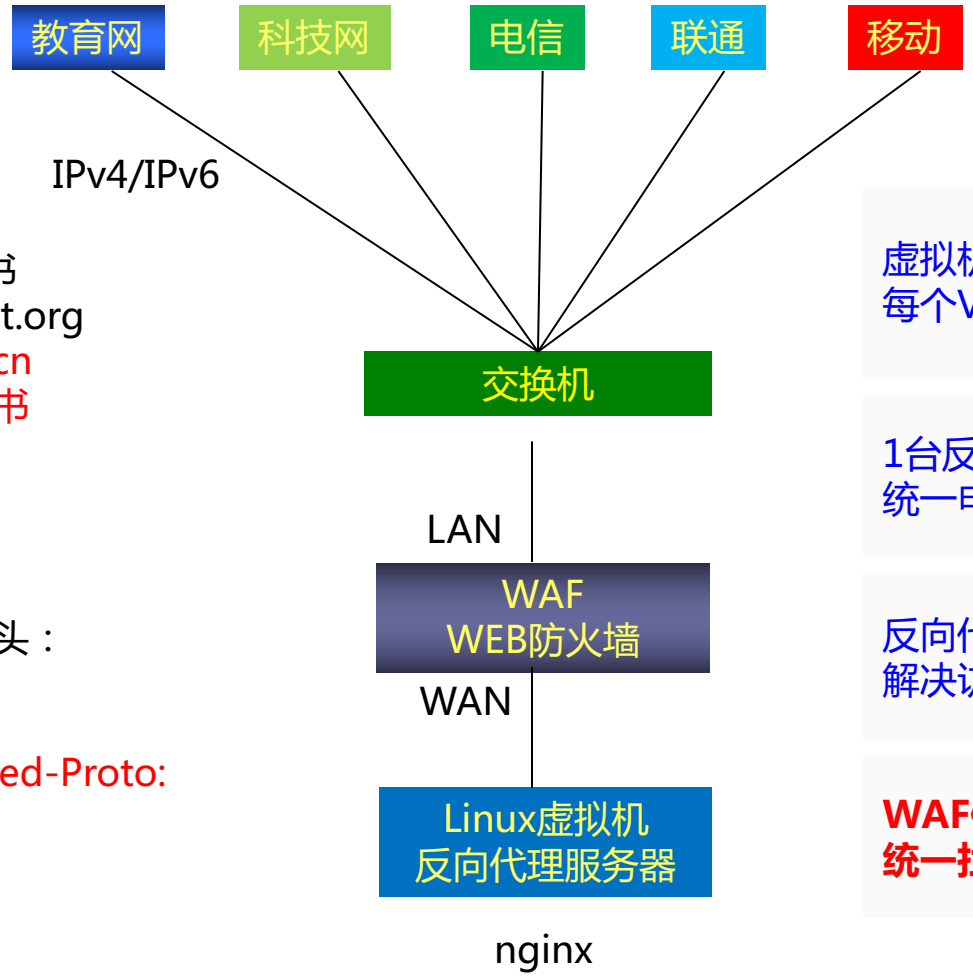
学校	IPv6	SSL	HTTP/2
Harvard University		●	●
MIT	●	●	
Stanford University		●	●
UC Berkeley	●	●	●
University of Oxford			
California Institute of Technology		●	
University of Cambridge		●	●
Columbia University		●	
Princeton University		●	
Yale University	●	●	●

C9学校主网站特性对比

https://www.17ce.com/ 2018年5月25日测试

学校	教育网	电信	联通	移动	鹏博士	IPv6	SSL	HTTP/2
中科大	●	●	●	●		●	●	●
北大	●	●	●		●			
清华	●					●		
浙大	●							
南大	●						●	
上交	●							
复旦	●							
西交	●							
哈工大			●					

IPV6+SSL网站服务



开源软件
免费证书
HTTP2支持

两种SSL证书
Letsencrypt.org
*.ustc.edu.cn
独立域名证书
自动更新

增加HTTP 头：
Host:
X-Real-IP:
X-Forwarded-Proto:

虚拟机1个接口划分若干VLAN
每个VLAN对应一个出口

1台反向代理服务600个网站
统一申请SSL证书+IPv6支持

反向代理服务器有6个入口
解决访问速度问题

WAF倒置
统一拦截各类WEB攻击

用户的跟踪与日志记录

采集交换机上的信息来跟踪用户

- 收集3层交换机用户的IPv6地址和MAC地址对应表
- show ipv6 nei
- 通过snmp协议收集2层交换机的MIB信息可以得到某个MAC地址是在哪个接口下的
- BRAS使用radius记账消息提供IPv6地址和MAC地址、2层VLAN的信息

使用这些信息，可以

- 任给IPv6地址，可以查出某个时间段对应的MAC地址
- 对于宿舍用户，根据内层VLAN号可以直接定位到宿舍房间
- 任给MAC地址，可以查出接在哪个交换机的哪个接口下

用户的跟踪与日志记录

IP	MAC	开始时间	结束时间	其他
2001:da8:d800:472:ec9d:bd48:d28b:f951(1/1/0)	18DBF261B646(255/232/48)	2018-04-13 00:10:40	2018-04-13 10:20:55	交换机端口
2001:da8:d800:144:358e:a03d:11ef:f7cf(1/1/0)	8CEC4B5A1451(663/170/0)	2018-04-12 22:00:10	2018-04-12 23:05:06	交换机端口
2001:DA8:D800:144:8578:31D2:4C09:BD7B(1/1/1)	B06EBF561D08(3493/169/54)	2017-10-12 22:27:01	2018-04-13 10:20:12	交换机端口
2001:da8:d800:472:846b:ec5d:eb1d:5c5d(1/1/0)	484D7E9D221C(1593/124/21)	2018-04-13 00:10:39	2018-04-13 10:20:55	交换机端口
2001:da8:d800:114:c16b:c328:e463:ce1f(1/1/0)	B06EBF6CE6A0(1835/97/34)	2018-04-13 00:00:27	2018-04-13 10:20:36	交换机端口
2001:da8:d800:195:d0c4:44d9:bff4:d1a6(1/1/0)	A888088C3892(317/97/0)	2018-04-12 21:45:33	2018-04-12 22:05:31	交换机端口
2001:da8:d800:148:1ccb:f9e4:6e0c:af8(1/1/0)	10604B7B5ECD(2688/91/12)	2018-04-13 00:10:30	2018-04-13 10:20:39	交换机端口
2001:da8:d800:195:d829:1aa8:6748:4f3f(1/1/0)	24F677490540(847/87/0)	2018-04-12 19:20:38	2018-04-12 19:40:38	交换机端口
2001:da8:d800:195:8564:7716:98a2:cd80(1/1/0)	00B3626925B3(366/86/14)	2018-04-12 22:00:35	2018-04-13 10:20:45	交换机端口
2001:da8:d800:195:e16d:e717:61ca:a904(1/1/0)	347C255B21EE(365/81/0)	2018-04-12 22:05:32	2018-04-12 22:25:34	交换机端口

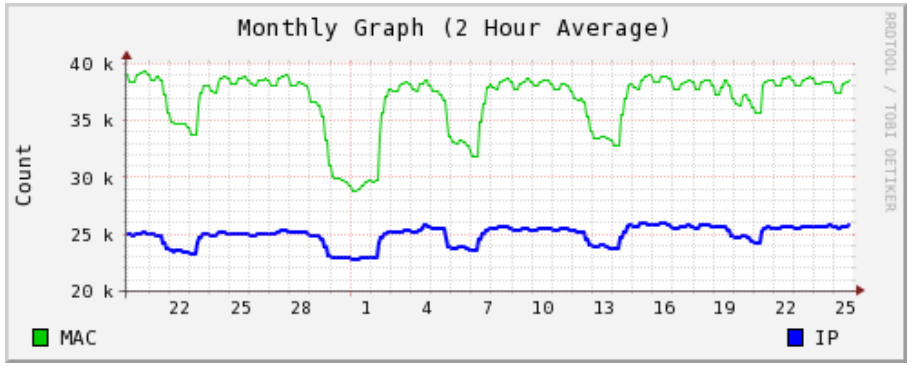
校园网IPV4/IPV6活动机器数据

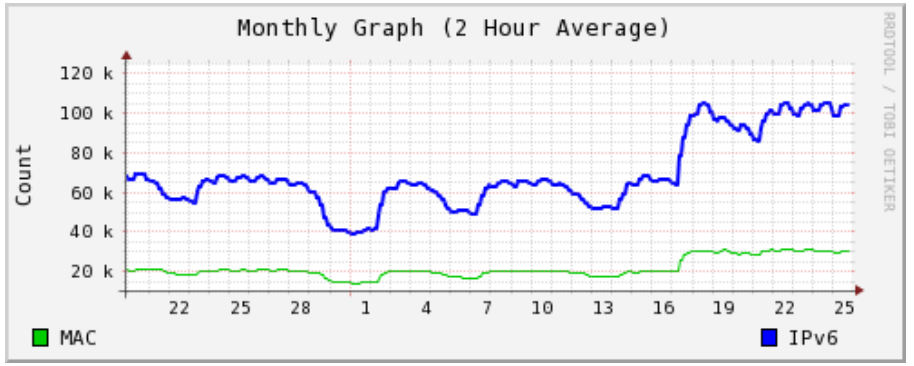
	IPv4机器数	IPv6机器数
一天内	4万	3万
一周内	6.9万	6.2万

IPv4机器数

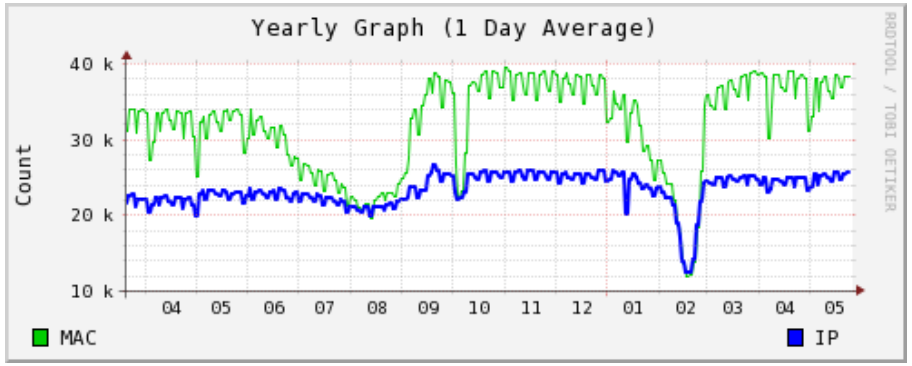
IPv6机器数

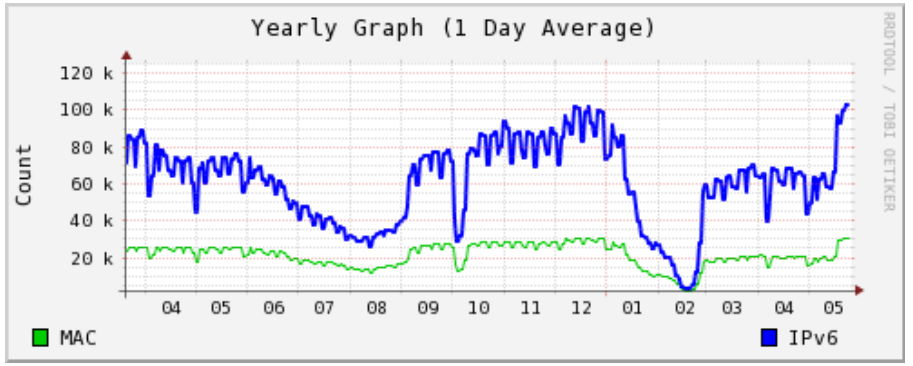
月



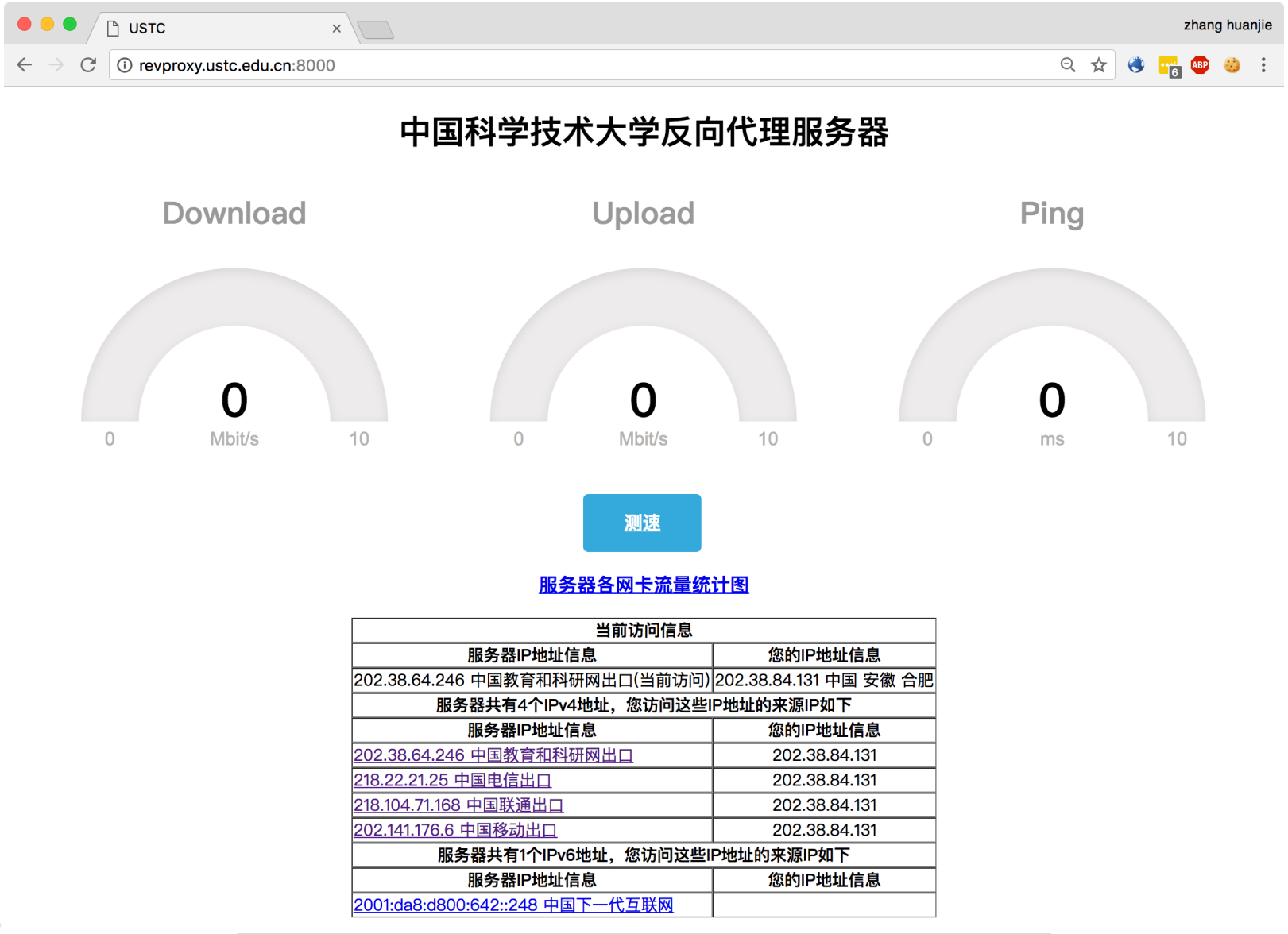


年



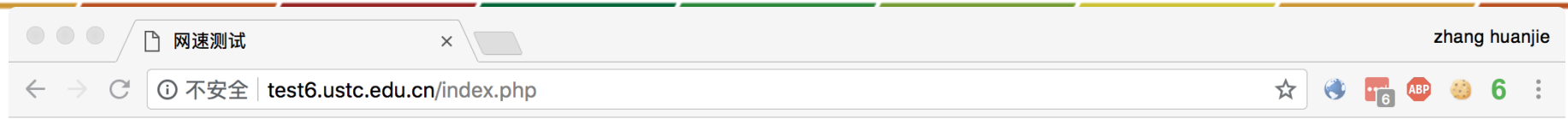


反向代理状态



当前访问信息	
服务器IP地址信息	您的IP地址信息
202.38.64.246 中国教育和科研网出口(当前访问)	202.38.84.131 中国 安徽 合肥
服务器共有4个IPv4地址，您访问这些IP地址的来源IP如下	
服务器IP地址信息	您的IP地址信息
202.38.64.246 中国教育和科研网出口	202.38.84.131
218.22.21.25 中国电信出口	202.38.84.131
218.104.71.168 中国联通出口	202.38.84.131
202.141.176.6 中国移动出口	202.38.84.131
服务器共有1个IPv6地址，您访问这些IP地址的来源IP如下	
服务器IP地址信息	您的IP地址信息
2001:da8:d800:642::248 中国下一代互联网	

测速网站



IPv4测速 http://test.ustc.edu.cn　IPv6测速 http://test6.ustc.edu.cn　另一种测速 speedtest　网络通登录

测试您访问中国科大测试站点的速度， 测试结果与网络速度和浏览器有关，仅供参考

您的IP地址是: 2001:da8:d800:642:f911:8580:a2c4:5ae3

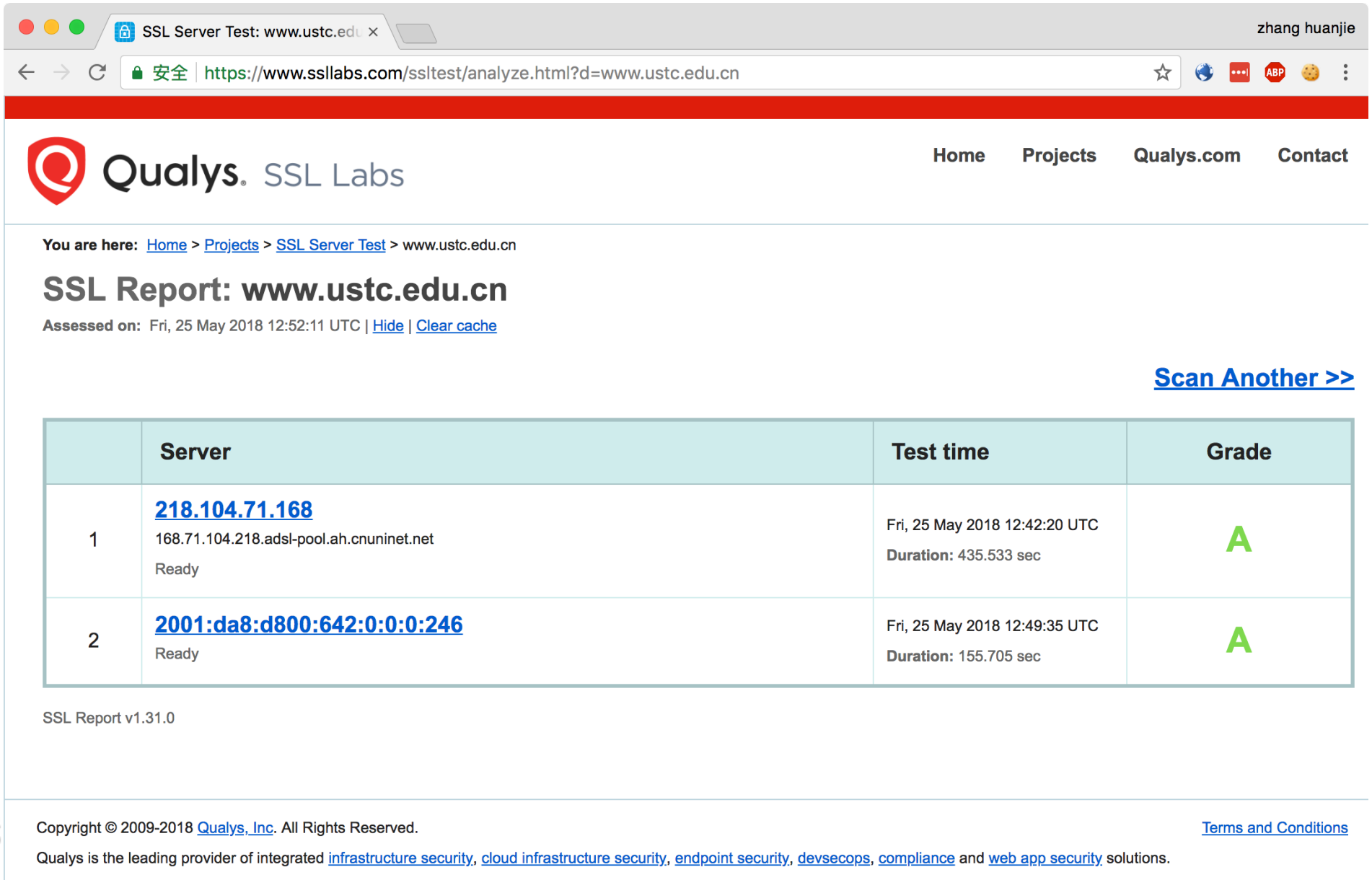
方向	测试结果	结果排行	建 议
下载	95.24Mbps	89.63%	网速飞快，恭喜你
上传	15.87Mbps	87.94%	网速正常

再测一次

近期测速信息

序号	IP	时间	下载速度Mbps	上传速度Mbps
1	2001:da8:d800:642:f911:8580:a2c4:5ae3	2018-08-14 10:45:48	95.24	15.87
2	2001:da8:d800:642:f911:8580:a2c4:5ae3	2018-08-14 10:45:46	95.24	18.69
3	2001:da8:d800:642:f911:8580:a2c4:5ae3	2018-08-14 10:45:35	102.57	19.23
4	202.38.64.207	2018-08-14 10:45:31	59.70	16.26
5	113.69.24.176	2018-08-14 10:43:49	2.32	0.46
6	113.69.24.176	2018-08-14 10:42:19	2.61	0.70
7	59.41.69.168	2018-08-14 10:41:37	5.34	0.86
8	114.214.173.229	2018-08-14 10:41:08	35.71	8.70
9	114.214.173.229	2018-08-14 10:41:06	32.52	9.57
10	114.214.173.229	2018-08-14 10:40:56	21.86	8.95
11	2001:da8:201:1412:7::3d	2018-08-14 10:39:14	0.44	0.18

网站访问SSL测试


SSL Server Test: www.ustc.edu
zhang huanjie
安全 | https://www.ssllabs.com/ssltest/analyze.html?d=www.ustc.edu.cn
Qualys. SSL Labs
Home
Projects
Qualys.com
Contact
You are here: Home > Projects > SSL Server Test > www.ustc.edu.cn
SSL Report: www.ustc.edu.cn
Assessed on: Fri, 25 May 2018 12:52:11 UTC | Hide | Clear cache
Scan Another >>
Server
Test time
Grade
1
218.104.71.168
168.71.104.218.adsl-pool.ah.cnuninet.net
Ready
Fri, 25 May 2018 12:42:20 UTC
Duration: 435.533 sec
A
2
2001:da8:d800:642:0:0:0:246
Ready
Fri, 25 May 2018 12:49:35 UTC
Duration: 155.705 sec
A
SSL Report v1.31.0
Copyright © 2009-2018 Qualys, Inc. All Rights Reserved.
Terms and Conditions
Qualys is the leading provider of integrated infrastructure security, cloud infrastructure security, endpoint security, devsecops, compliance and web app security solutions.

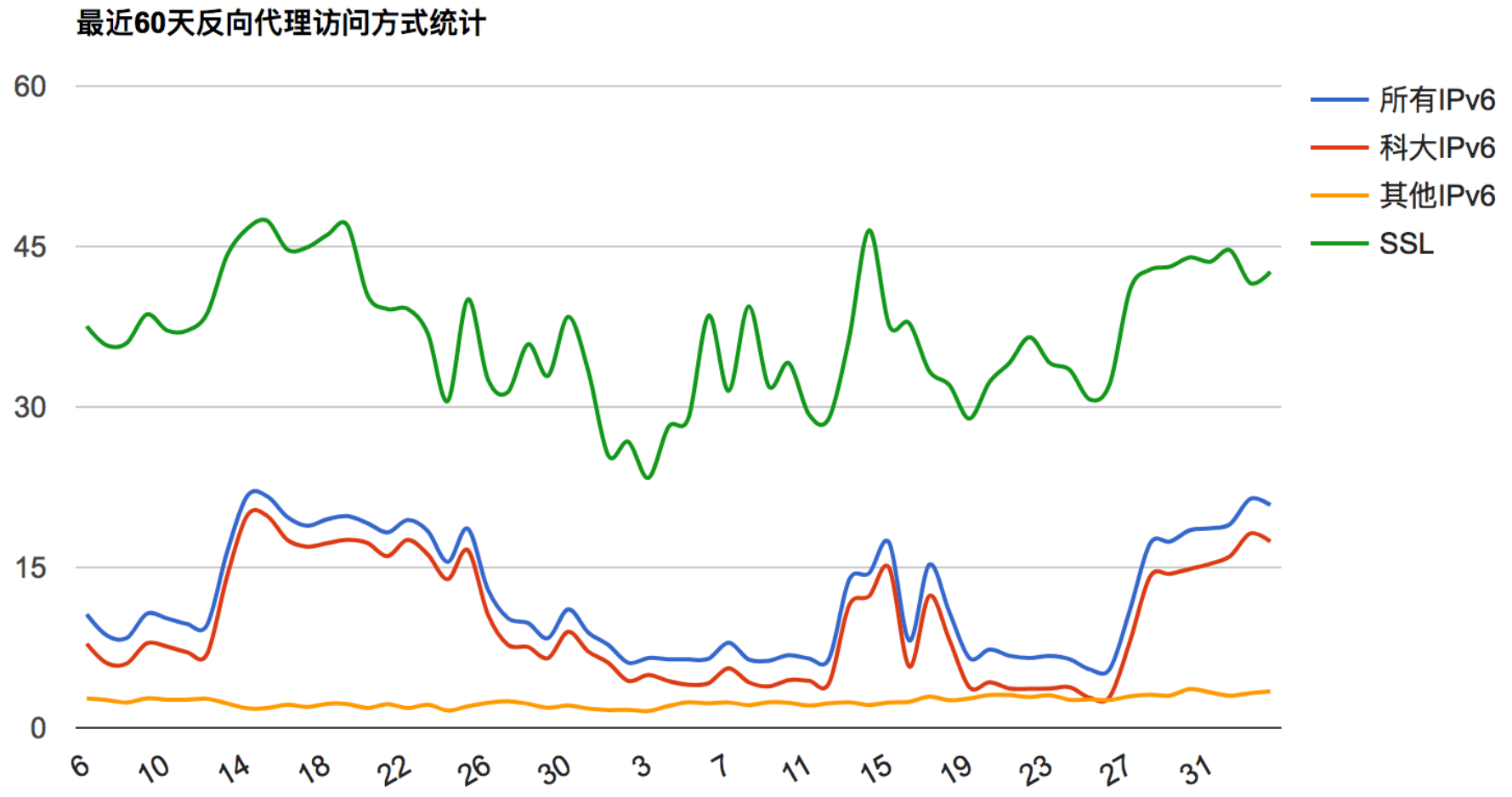
网站访问统计

反向代理访问统计图 2018-05-25

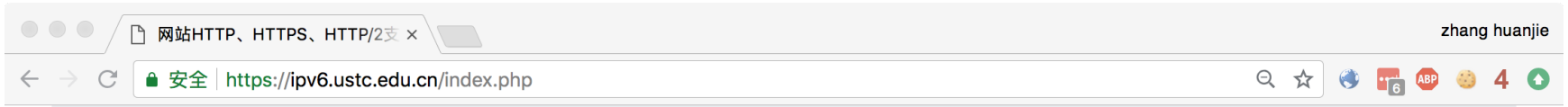
主机	总数	IPv4	IPv4比例	IPv6	IPv6比例	校内IPv6	校内IPv6比例	校外IPv6	校外IPv6比例	SSL	SSL比例
www.ustc.edu.cn	442400	398405	90.1%	43995	9.9%	33890	7.7%	10105	2.3%	2130	0.5%
imicro.ustc.edu.cn	304929	296984	97.4%	7945	2.6%	4024	1.3%	3921	1.3%	290	0.1%
pyxt.ustc.edu.cn	223009	156398	70.1%	66611	29.9%	57443	25.8%	9168	4.1%	69	0.0%
yz.ustc.edu.cn	169007	158126	93.6%	10881	6.4%	2701	1.6%	8180	4.8%	889	0.5%
yjs.ustc.edu.cn	162427	130274	80.2%	32153	19.8%	29657	18.3%	2496	1.5%	2767	1.7%
news.ustc.edu.cn	153020	137665	90.0%	15355	10.0%	11970	7.8%	3385	2.2%	610	0.4%
www.zkdfz.com	144188	144188	100.0%	0	0.0%	0	0.0%	0	0.0%	55	0.0%
mis.teach.ustc.edu.cn	138466	115487	83.4%	22979	16.6%	22182	16.0%	797	0.6%	263	0.2%
tqms.ustc.edu.cn	102386	87577	85.5%	14809	14.5%	516	0.5%	14293	14.0%	181	0.2%
xly.ustc.edu.cn	95122	82693	86.9%	12429	13.1%	318	0.3%	12111	12.7%	1265	1.3%
www.teach.ustc.edu.cn	90851	77211	85.0%	13640	15.0%	13059	14.4%	581	0.6%	82799	91.1%
gradschool.ustc.edu.cn	85557	71880	84.0%	13677	16.0%	9624	11.2%	4053	4.7%	1377	1.6%
zsb.ustc.edu.cn	79875	77346	96.8%	2529	3.2%	1091	1.4%	1438	1.8%	976	1.2%
finance.ustc.edu.cn	71271	51342	72.0%	19929	28.0%	19493	27.4%	436	0.6%	51	0.1%
ustc.edu.cn	67768	59508	87.8%	8260	12.2%	4475	6.6%	3785	5.6%	622	0.9%
www.job.ustc.edu.cn	64497	54334	84.2%	10163	15.8%	9182	14.2%	981	1.5%	1010	1.6%
hospital.ustc.edu.cn	64372	63288	98.3%	1084	1.7%	1040	1.6%	44	0.1%	9	0.0%
epc.ustc.edu.cn	55613	45726	82.2%	9887	17.8%	9821	17.7%	66	0.1%	86	0.2%
www.hfnl.ustc.edu.cn	55468	40923	73.8%	14545	26.2%	12873	23.2%	1672	3.0%	420	0.8%
hsss.ustc.edu.cn	54765	53982	98.6%	783	1.4%	507	0.9%	276	0.5%	79	0.1%
business.ustc.edu.cn	53481	46044	86.1%	7437	13.9%	4724	8.8%	2713	5.1%	163	0.3%

网站访问统计

https://linux.ustc.edu.cn/web/



网站监测与测试 https://ipv6.ustc.edu.cn/



网站HTTP、HTTPS、HTTP/2支持情况

[相关说明 | 测试历史 | 分组对比 | 得分变化]

[所有网站(47.6) | 国际知名高校(62.5) | 九校联盟高校(65.6) | 一流大学高校(57.3) | 一流学科高校(45.2) | 其他高校(66.9) | 安徽省高校(45.8) | 港澳台高校(53.8) | CDN厂商(59.0) | 互联网企业(62.7) | 媒体(39.3) | C9招生网(47.8)]

https://ipv6.ustc.edu.cn 由 中国科学技术大学网络信息中心 提供，每30分钟运行一次

让网站全面支持v4/v6 HTTP、HTTPS、HTTP/2最简单方法是增加Nginx反向代理服务器，https://github.com/bg6cq/nginx-install 有详细安装说明

请输入主机名： www.ustc.edu.cn 开始测试 最后100条在线测试结果 在线测试次数排行

测试时间：2018-09-03 21:20:47

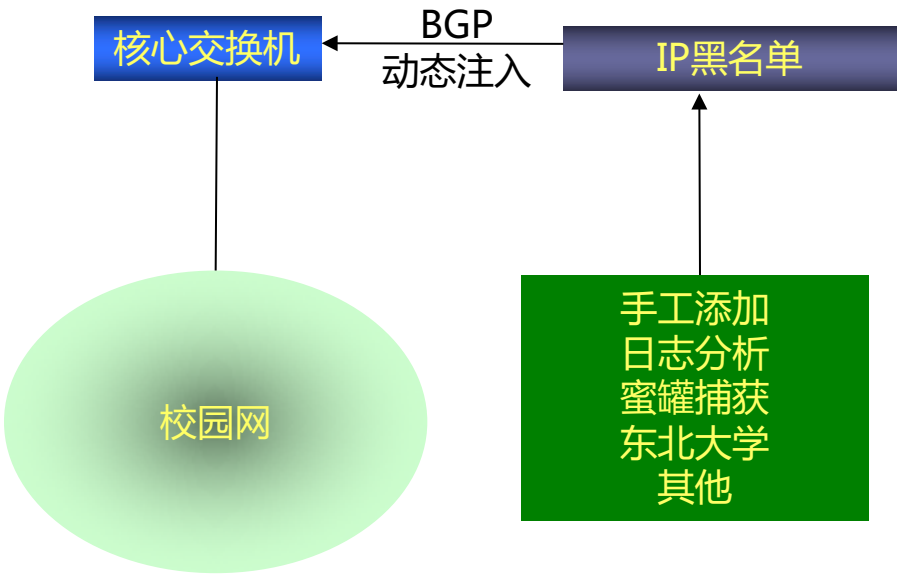
所有网站 测试历史 不稳定排行

Search:

	单位	网站	v4 HTTP	v4 HTTPS	v4 HTTP2	v6解析	v6 HTTP	v6 HTTPS	v6 HTTP2	评分
1	耶鲁	www.yale.edu	✔	✔	✔	✔	✔	✔	✔	127
2	中国科学技术大学	www.ustc.edu.cn	✔	✔	✔	✔	✔	✔	✔	126

ZERO TRUST

IP黑名单系统—直接封禁IP



原理：

ip route 192.0.2.1/32 Null0

ipv6 route 2001:db8::1/128 Null0

通过BGP把黑名单IP的next_hop设置为
192.0.2.1或2001:db8::1

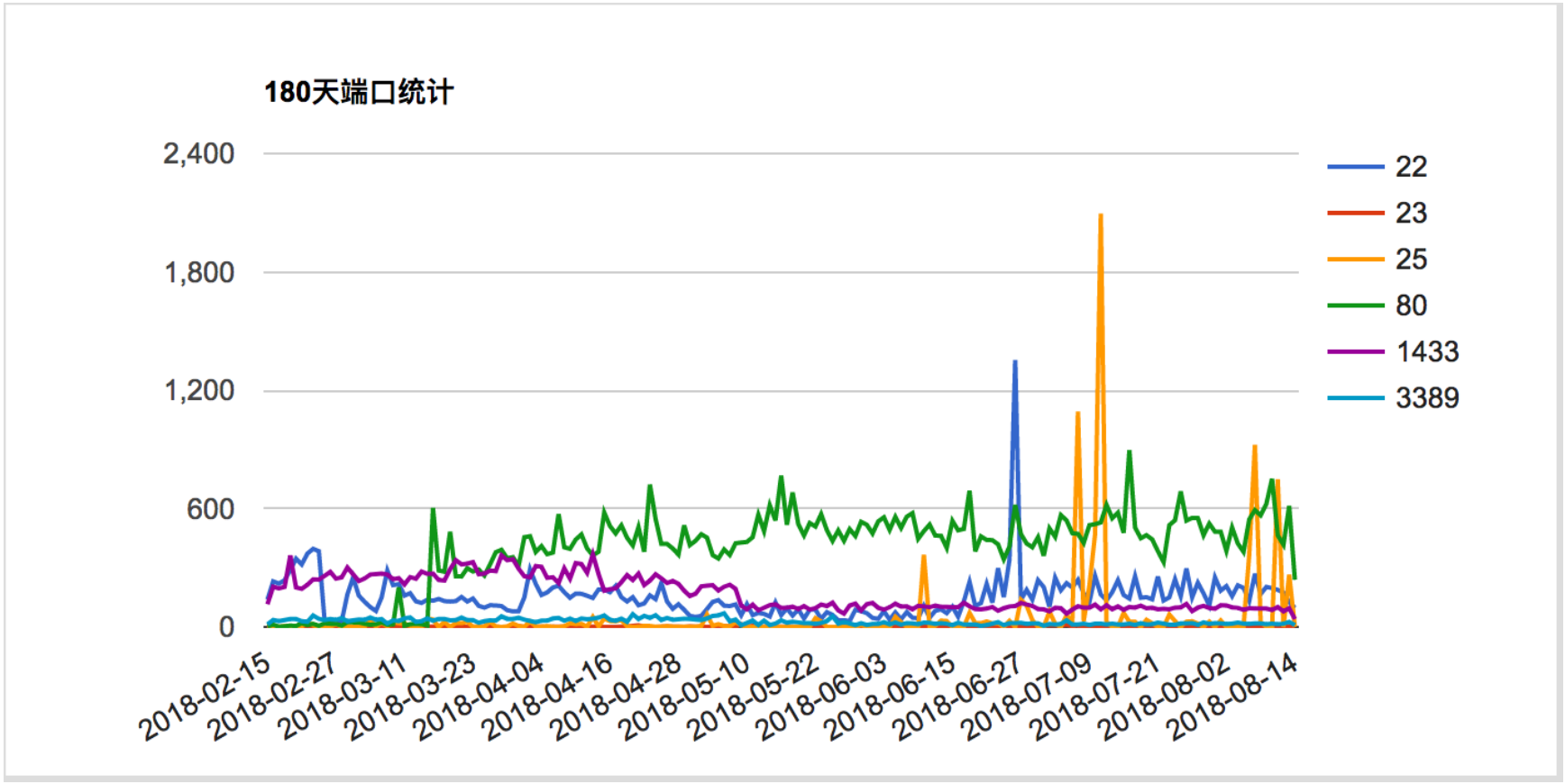
IP黑名单系统
http://blackip.ustc.edu.cn

丢弃发给黑名IP的数据包（单向）

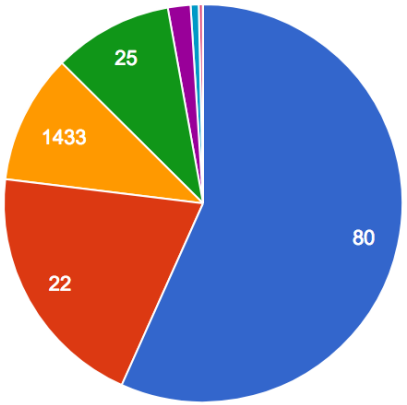
0022 ssh扫描
0023 telnet扫描
0025 垃圾邮件发送
0080 恶意文件下载、WAF报警
1433 SQL扫描
3306 MySQL扫描
3389 远程桌面扫描

不同的攻击，加黑名单的时间不等

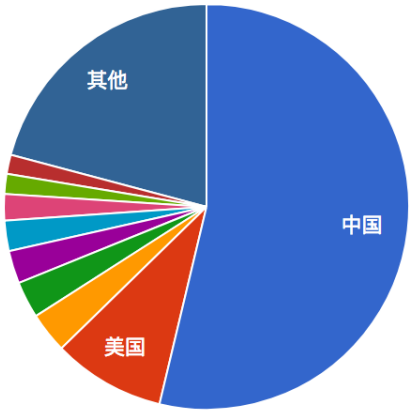
黑名单IP统计



10大威胁端口



攻击来源



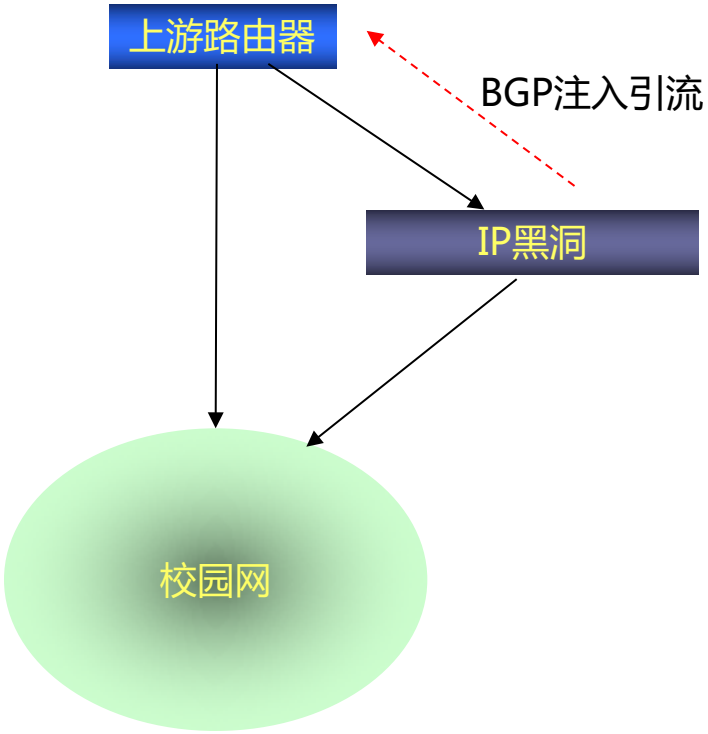
IP黑名单管理

封锁时间	失效时间	IP地址	说明	IP信息
2018-04-13 15:14:02	2018-05-13 15:19:02	158.69.32.43	0023 scan ahernet	加拿大 加拿大
2018-04-13 15:12:25	2018-04-13 16:12:25	116.226.90.15	0080 WAF Apr13 15:11:27	中国 上海 上海
2018-04-13 15:11:41	2018-04-13 20:11:41	210.16.189.4	0080 WAF Apr13 15:10:42	中国 上海 上海
2018-04-13 15:10:03	2018-04-18 15:10:03	218.64.216.99	1433 scan xc-ls	中国 江西 赣州
2018-04-13 15:10:02	2018-04-18 15:10:02	110.87.105.144	1433 scan xc-ls	中国 福建 厦门
2018-04-13 15:10:02	2018-04-18 15:10:02	122.114.52.98	1433 scan xc-ls	中国 河南 郑州
2018-04-13 15:09:31	2018-04-13 16:09:31	81.169.144.135	0080 WAF Apr13 15:08:32	德国 德国
2018-04-13 15:06:39	2018-04-13 20:06:39	2002:893b:9513::893b:9513	0080 WAF Apr13 15:05:40	ipv6
2018-04-13 15:03:31	2018-04-13 20:03:31	142.4.104.172	0080 WAF Apr13 15:02:33	美国 美国
2018-04-13 15:02:01	2018-04-13 16:02:01	171.106.197.245	0080 WAF Apr13 15:01:03	中国 广西 贵港
2018-04-13 15:01:58	2018-04-13 20:01:58	183.156.246.188	0080 WAF Apr13 15:01:00	中国 浙江 杭州
2018-04-13 15:00:04	2018-04-18 15:00:04	121.28.0.163	1433 scan xc-ls	中国 河北 石家庄
2018-04-13 15:00:04	2018-04-18 15:00:04	124.205.183.44	1433 scan xc-ls	中国 北京 北京
2018-04-13 15:00:03	2018-04-18 15:00:03	5.188.10.168	3389 scan xc-ls	保加利亚 保加利亚
2018-04-13 15:00:03	2018-04-18 15:00:03	213.32.37.16	3389 scan xc-ls	法国 法国
2018-04-13 15:00:02	2018-04-18 15:00:02	1.52.195.223	1433 scan xc-ls	越南 越南
2018-04-13 14:58:16	2018-04-13 15:58:16	183.160.238.195	0080 WAF Apr13 14:57:17	中国 安徽 合肥
2018-04-13 14:50:03	2018-04-18 14:50:03	218.64.216.79	1433 scan xc-ls	中国 江西 赣州
2018-04-13 14:50:02	2018-04-18 14:50:02	125.78.32.16	1433 scan xc-ls	中国 福建 泉州
2018-04-13 14:44:17	2018-04-13 19:44:17	240e:f0:44:4f07:44af:2c98:ad1d:1e5a	0080 WAF Apr13 14:43:19	ipv6
2018-04-13 14:41:58	2018-04-13 19:41:58	137.59.149.19	0080 WAF Apr13 14:41:00	中国 香港
2018-04-13 14:40:01	2018-04-23 14:40:01	118.89.29.169	0023 scan 95.67.kirpa	中国 广东 广州

IP黑名单管理


详细信息
攻击行为名称:
下载关键文件
拦截原因:
1400001
URL:
http://physics.ustc.edu.cn/HYTop.mdb
数据长度:
271
攻击时间:
2018-04-13 15:05:40
源IP地址:
2002:893b:9513::893b:9513
目的IP地址:
202.38.64.115
危害等级:
中等
事件描述:
防止下载mdb数据库文件、*.inc文件、*.config文件
mdb是Microsoft Access软件使用的一种存储格式,因其对数据操作的方便性,常用在一些中小型程序中；
inc一般是include文件格式,用于编写复用代码的，比如在脚本编写过程中把很多页面需要运用的自定义代码统一写在一个inc文件中然后用include语句包含
解决方案:
临时解决方法：
对于.mdb、.inc、.config等后缀，可在IIS中设置一个该后缀的扩展映射，将这个映射使用一个无关的dll文件来防止该后缀的文件被下载。这样不仅可以解决该漏洞问题，还可以避免其他很多安全问题。

IP黑洞系统—封禁对校内的流量



通过BGP把需要引流IP的next_hop
设置为IP黑洞的IPv4或v6地址

IP黑洞系统
http://blackhole.ustc.edu.cn

作用：丢弃发给某IP所有或特定数据包（单向）

扫描找出校内有安全隐患的IP或IP的端口
黑洞系统通过BGP协议进行引流
黑洞系统将数据包过滤后送给校园网

自动化、高效率封禁对校内的部分流量

自动规则：
所有启用反向代理服务的IP 80端口
所有摄像头IP
所有校内打印机IP
所有服务器IPMI IP
服务器网段的3389端口
所有探测到的53端口
所有探测到的1433/1521/3306等端口

存在问题与下一步工作思考

如何认证计费最方便？

- 无线网依赖eduroam，802.1X接入认证，可以解决认证问题
- 有线网络倾向使用与目前v4类似的出口portal认证
- 越来越多的https网站，使得portal弹窗越来越不方便

如何使用多家运营商出口？

- 理想中的BGP能实现吗？BGP能完美解决选路问题吗？
- 如果不能实现，是否需要目前v4的用户自主选择出口？
- 多家运营商出口还需要NAT吗？

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国·北京

Internet Security Conference 2018 Beijing·China

（原中国互联网安全大会）