

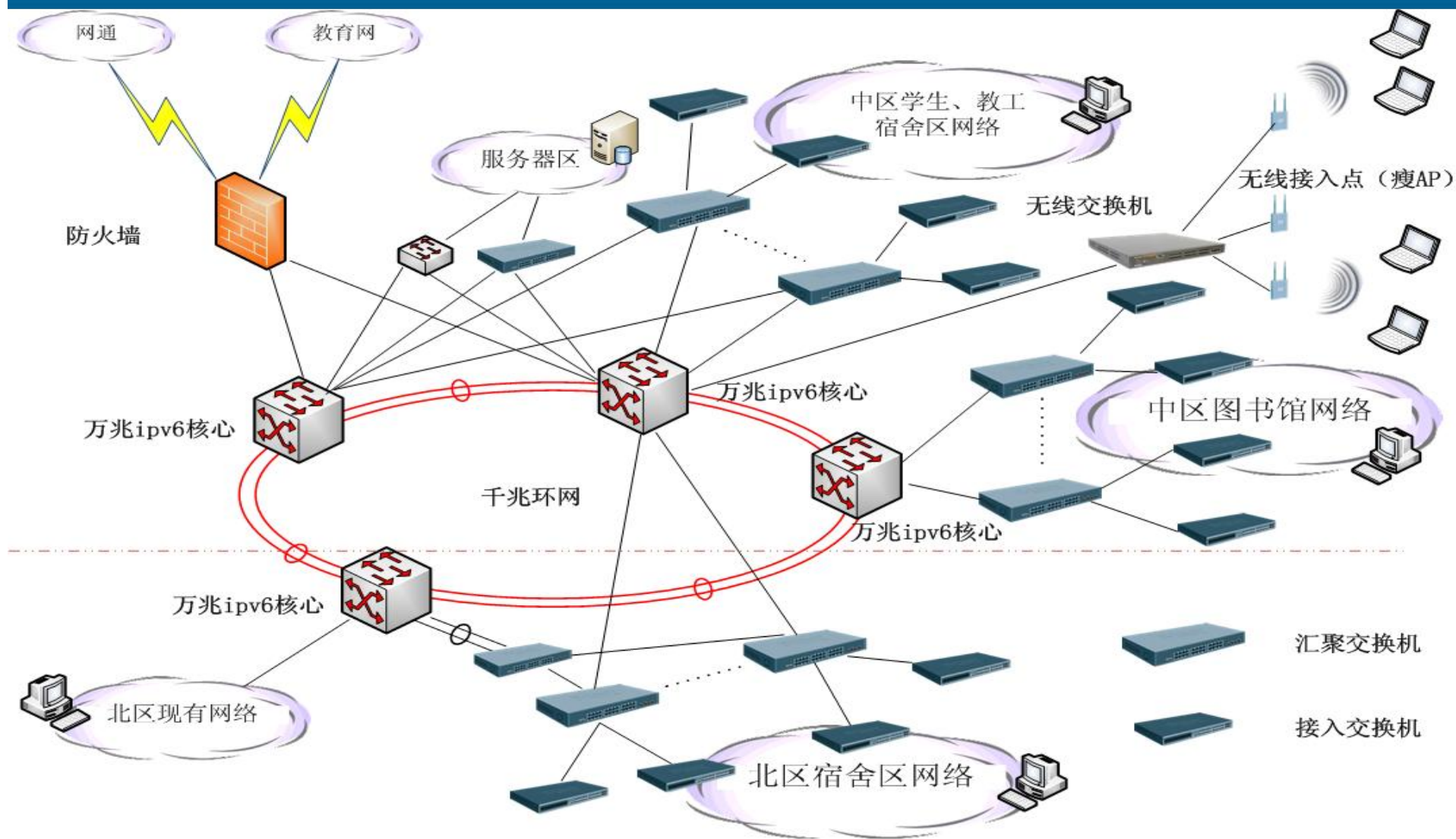


高校数字化校园可持续化良性运营

-----D-Link校园网运营升级改造方案

董良

中型校园网典型拓扑



现有网络面临的一些问题和挑战

- 1、ARP攻击及病毒泛滥，常常引起大面积上网中断
- 2、用户上网行为不可控（乱发言论、乱用网络资源现象严重）
- 3、学生区、家属区用户要大量接入网络，给我们的网络运营带来不小的挑战。（防代理、防私接，同时还要保障用户正常的网络访问速度不低于运营商）

目标

- 1、双向防御ARP攻击及病毒对网络的侵犯
- 2、对用户的上网行为进行有效的控制
- 3、全面、丰富的认证计费计费手段

让我们的网络环境更舒适、更安全

一、双向防御ARP攻击及病毒对网络的侵犯

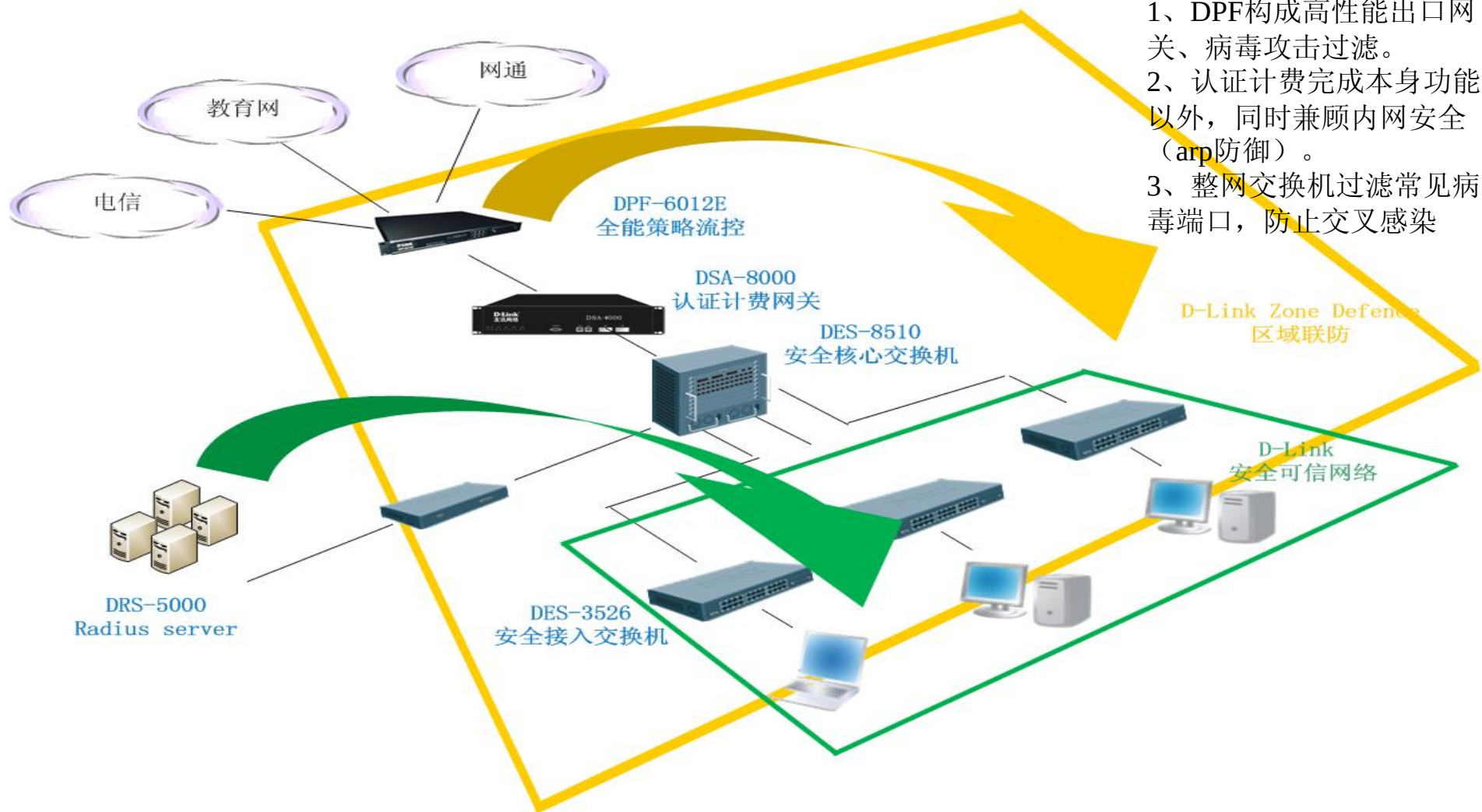
原因

导致用户上网掉线的最大原因就是arp攻击
其次是病毒等的攻击
最后是网络本身的瓶颈问题



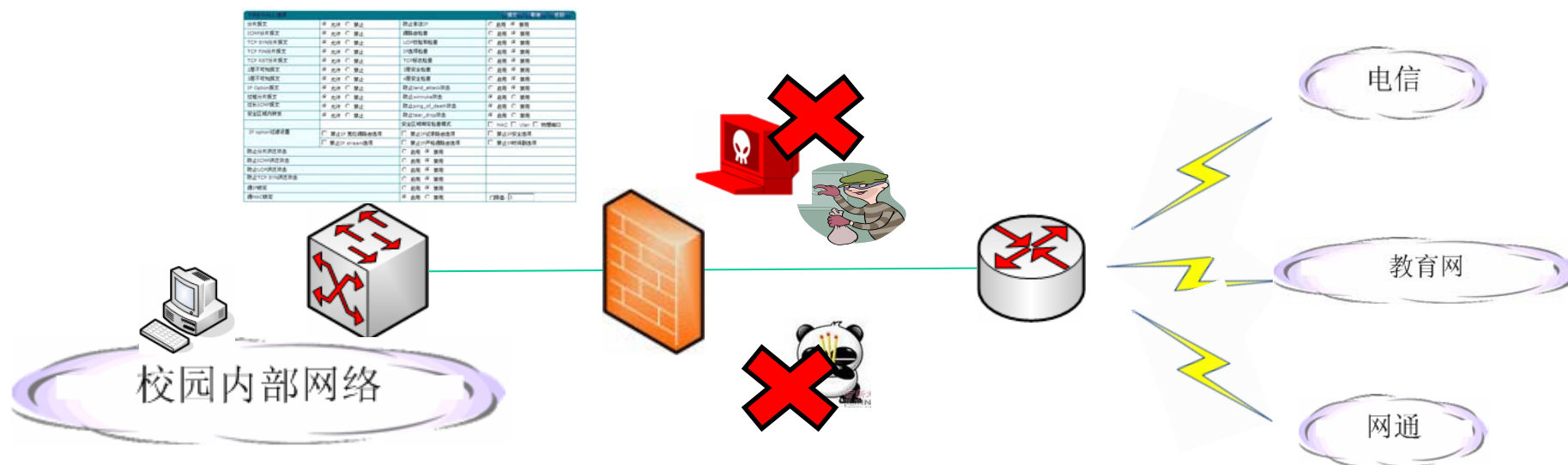
上网不稳定
总是掉线

方案逻辑拓扑



- 1、DPF构成高性能出口网关、病毒攻击过滤。
- 2、认证计费完成本身功能以外，同时兼顾内网安全（arp防御）。
- 3、整网交换机过滤常见病毒端口，防止交叉感染

增加安全防御设备（防火门）-----防外



抑制各种安全威胁（各种扫描、DOS、DDOS等攻击）
同时要对内部开放的应用进行认证（禁止非授权应用）

Arp的防范

单一的IP+MAC+端口绑定，DHCP snooping都不能完全解决问题
我们需要：

认证计费客户端、交换机、radius server

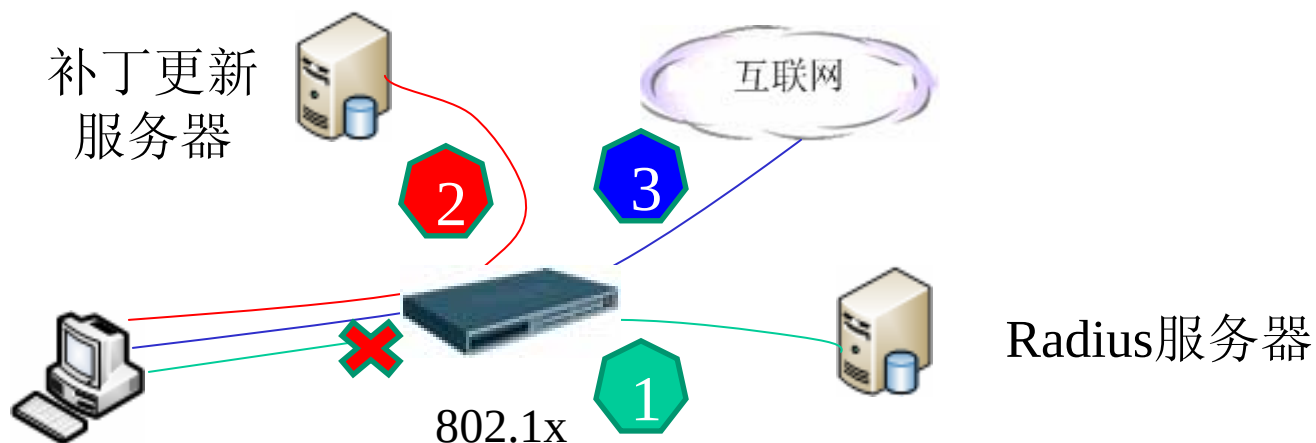
组成三位一体，共同完成对arp攻击的防御

- 1、认证前会有一个arp防御的小程序驻留在系统内，对发出的arp进行有效的侦测和隔离
- 2、认证开始后，客户端清除arp后，会用所使用的网卡发送arp，并进行绑定
- 3、每15秒，会发一次arp，帮助网关维护arp
- 4、这个过程中radius server要对用户的ip进行绑定

补丁更新、病毒防范

- 1、通过在网络设备上关闭常见的病毒端口，切断扫描通道
- 2、在网络上部署IPS功能的设备进行攻击预防
- 3、和杀毒软件进行联合，形成三位一体的防御工事

认证计费客户端内建安全检查功能，系统补丁、杀毒软件等不符合预定义的安全策略的主机不能访问网络



二、对用户的上网行为进行有效的控制

- 1、所有用户访问网络资源的行为要记录（海量日志记录）
- 2、一些发布有害信息的地方要屏蔽（类似百度贴吧的网站进行屏蔽）
- 3、用户使用的应用要控制（应用识别、智能带宽保障）

整个系统要能灵活、合理的保障出口带宽的最大化

应用保障

- 1、应用灵活的策略增加带宽的利用率
- 2、对关键应用进行有效的保障
- 3、对非关键应用进行合理的控制

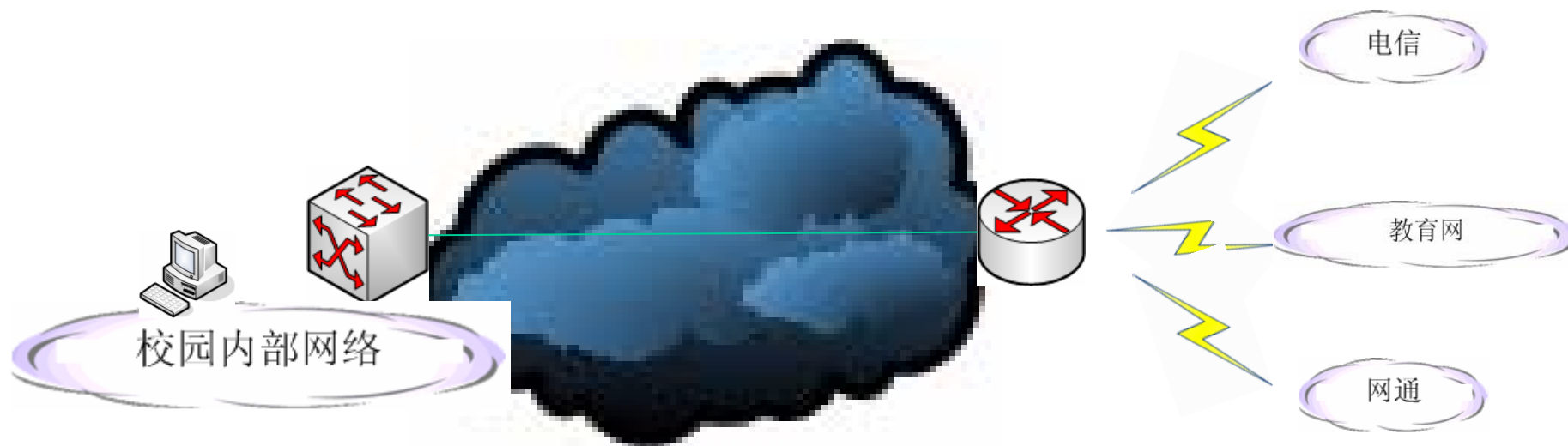
[illegible][illegible]

邮件记录

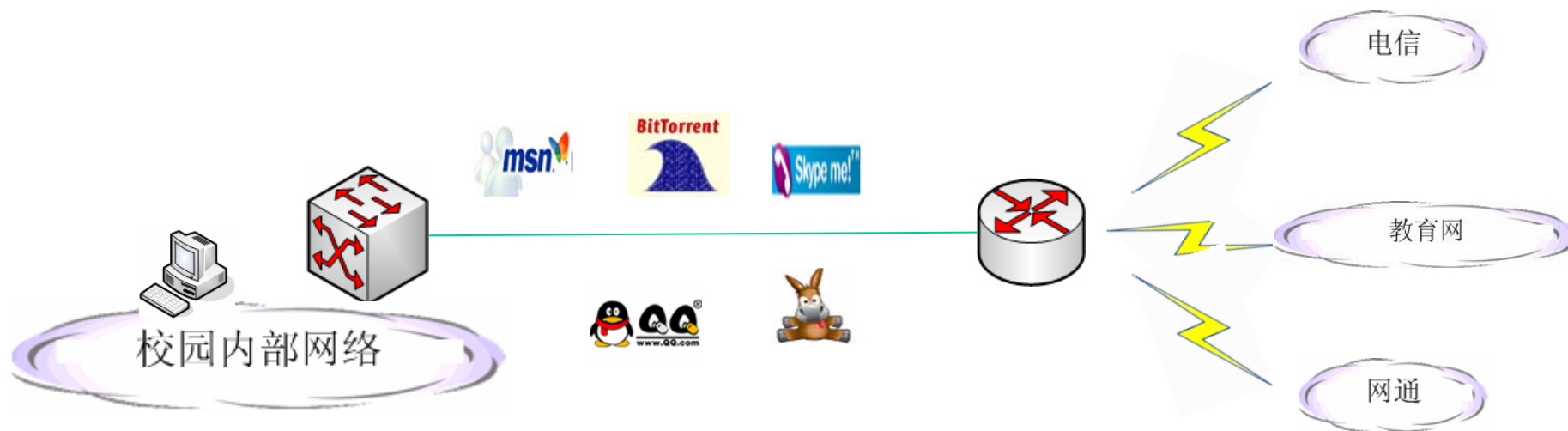
[illegible]

URL记录

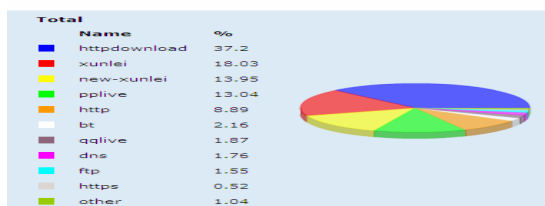
网络应用不可识别（黑匣子）



网络流量的可视化（拨云见日）

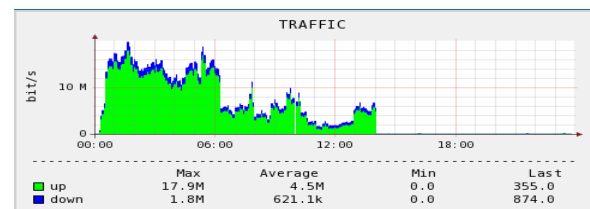


总流量 前十名



会话日志

序号	设备	源IP	源端口	目的IP	目的端口	协议	应用	流量	时间
会话记录数: 23743975 待过滤记录数: 23743975									
1	DFF-00120	172.28.17.3	2348	202.202.144.8	21	6	1	202.196.109.3	40804
2	DFF-00120	202.196.98.86	2443	61.226.75.77	21	6	1	218.28.30.197	27906
3	DFF-00120	190.38.176.24	1788	218.186.194.8	21	6	0	0.0.0.0	0
4	DFF-00120	121.236.96.203	3572	218.186.55.79	21	6	0	0.0.0.0	0
5	DFF-00120	202.196.103.12	1803	158.211.218.20	21	6	1	202.196.109.2	7944
6	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
7	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
8	DFF-00120	202.196.103.12	1803	158.211.218.20	21	6	1	202.196.109.2	7944
9	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
10	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
11	DFF-00120	202.202.85.205	4863	202.196.103.97	21	6	0	0.0.0.0	0
12	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
13	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
14	DFF-00120	172.28.17.3	2342	202.202.144.8	21	6	1	202.196.109.3	40804
15	DFF-00120	211.81.21.82	49581	202.196.103.97	21	6	0	0.0.0.0	0
16	DFF-00120	128.219.32.211	7918	202.196.103.97	21	6	0	0.0.0.0	0
17	DFF-00120	61.233.17.140	14029	218.186.194.8	21	6	0	0.0.0.0	0
18	DFF-00120	121.30.292.78	10300	218.186.48.21	21	6	0	0.0.0.0	0
19	DFF-00120	172.24.21.12	1080	182.148.8.252	21	6	1	202.196.109.2	7944
20	DFF-00120	124.128.148.2	6301	218.186.48.21	21	6	0	0.0.0.0	0
21	DFF-00120	172.24.21.12	1080	182.148.8.252	21	6	1	202.196.109.2	7944
22	DFF-00120	202.196.103.12	1803	158.211.218.20	21	6	1	202.196.109.2	7944
23	DFF-00120	60.7.211.213	30489	202.196.103.97	21	6	0	0.0.0.0	0



识别方法发展



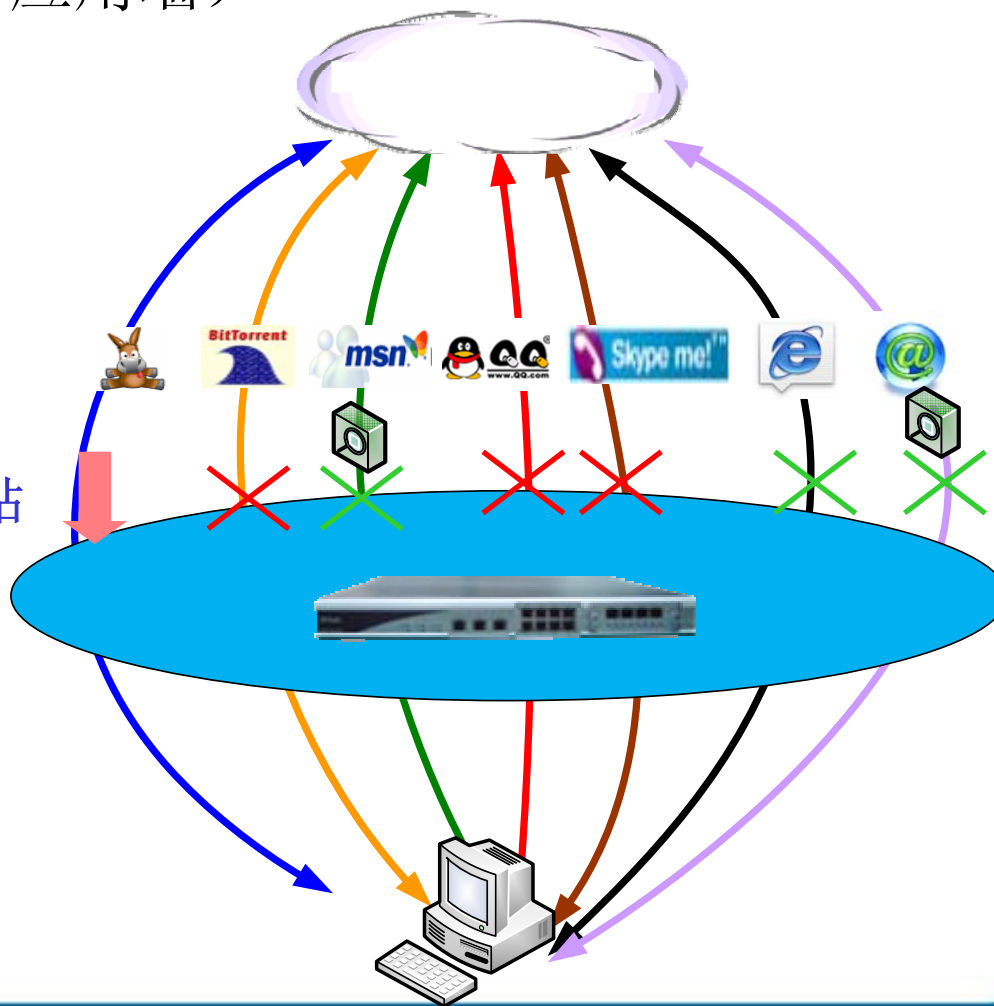
丰富手段进行用户行为管理（应用墙）



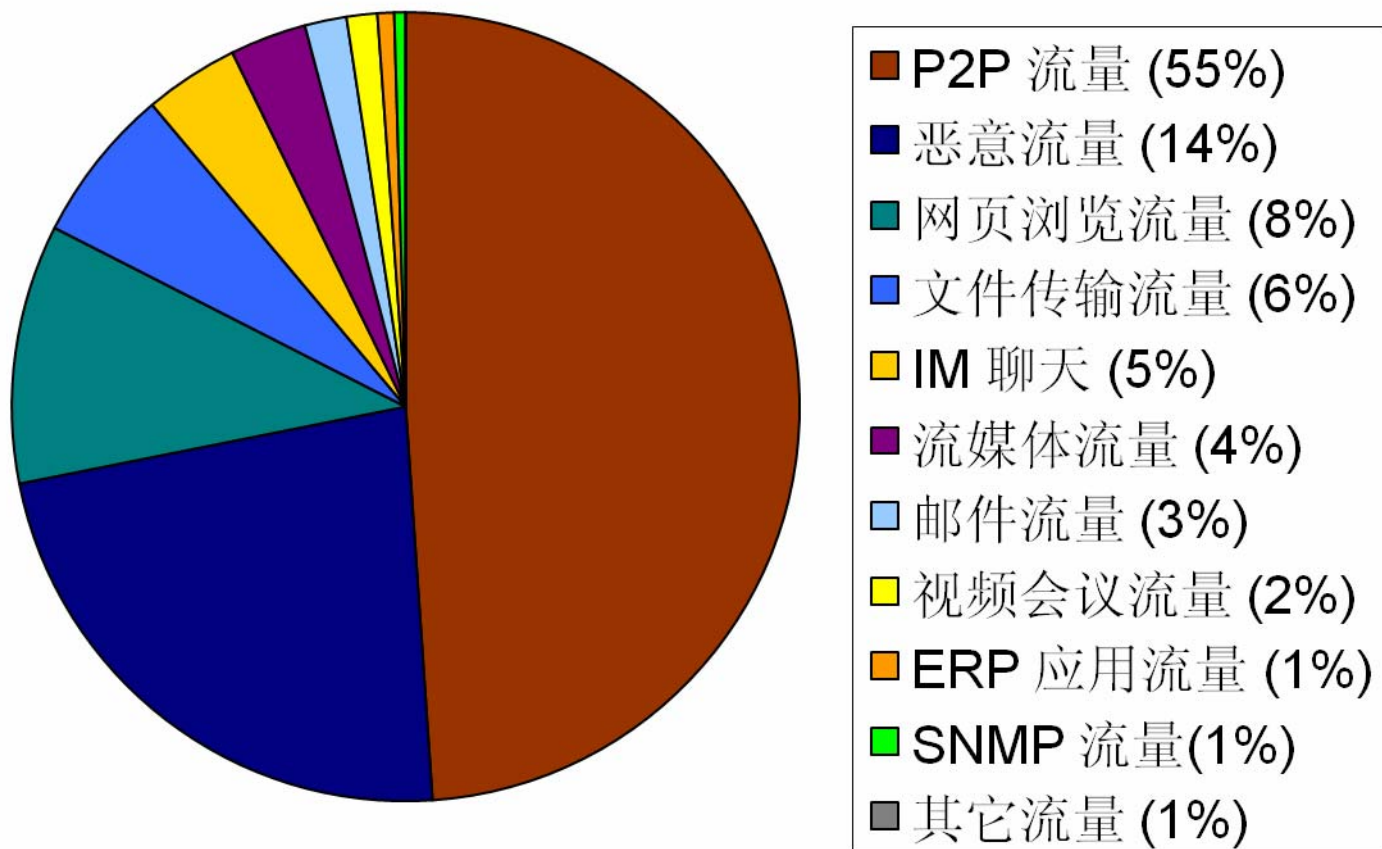
对URL进行特征字过滤，过滤不良网站 脚本、文件等过滤

允许MSN聊天, 不允许传文件和视频

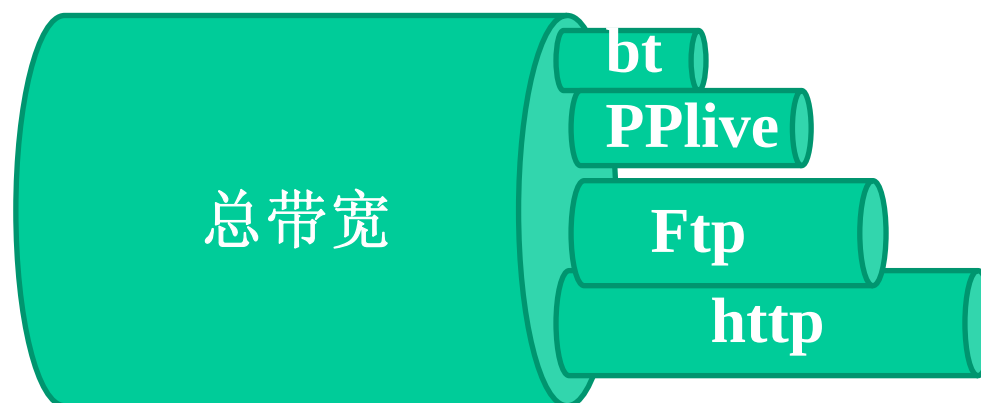
允许收发Email, 不允许加附件



P2P等应用对带宽的侵蚀



基于IP、应用 的智能带宽保障（灵活调度）



每种应用根据最小、保障、最大三种阈值进行带宽适配

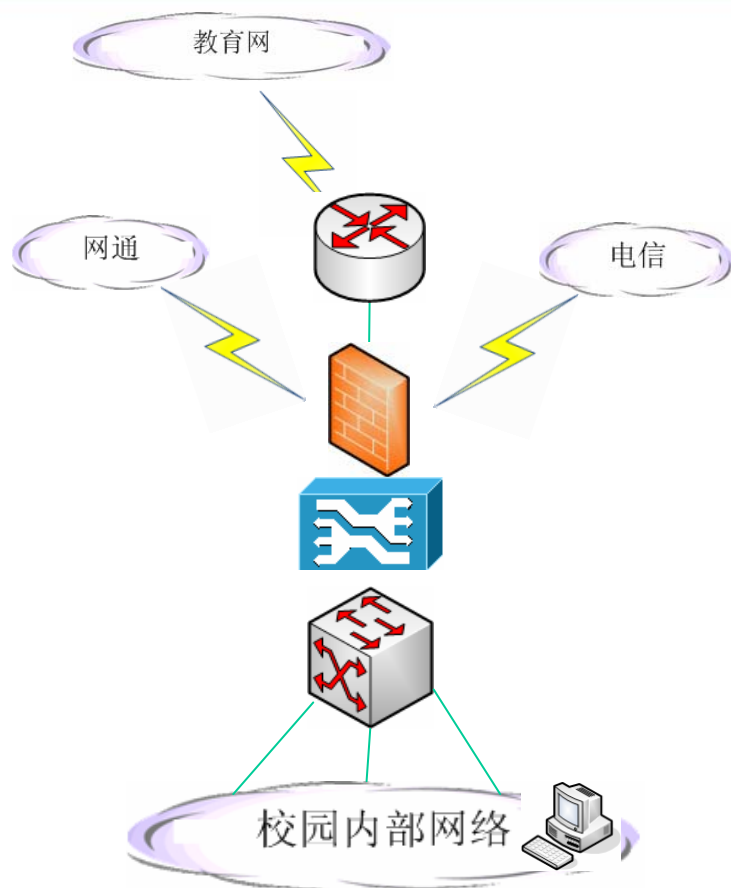
最小带宽 （专用车道）

保障带宽 （超车道）

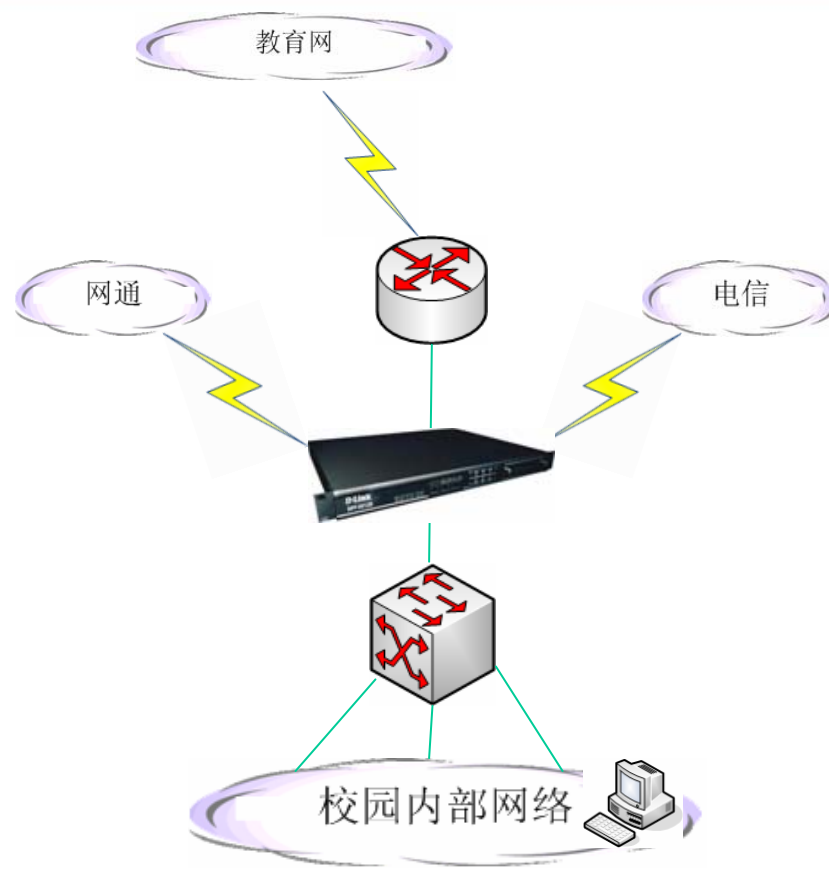
最大带宽 （限速牌）

保障重要应用、抑制P2P

传统流控和综合流控设备对比



传统流控



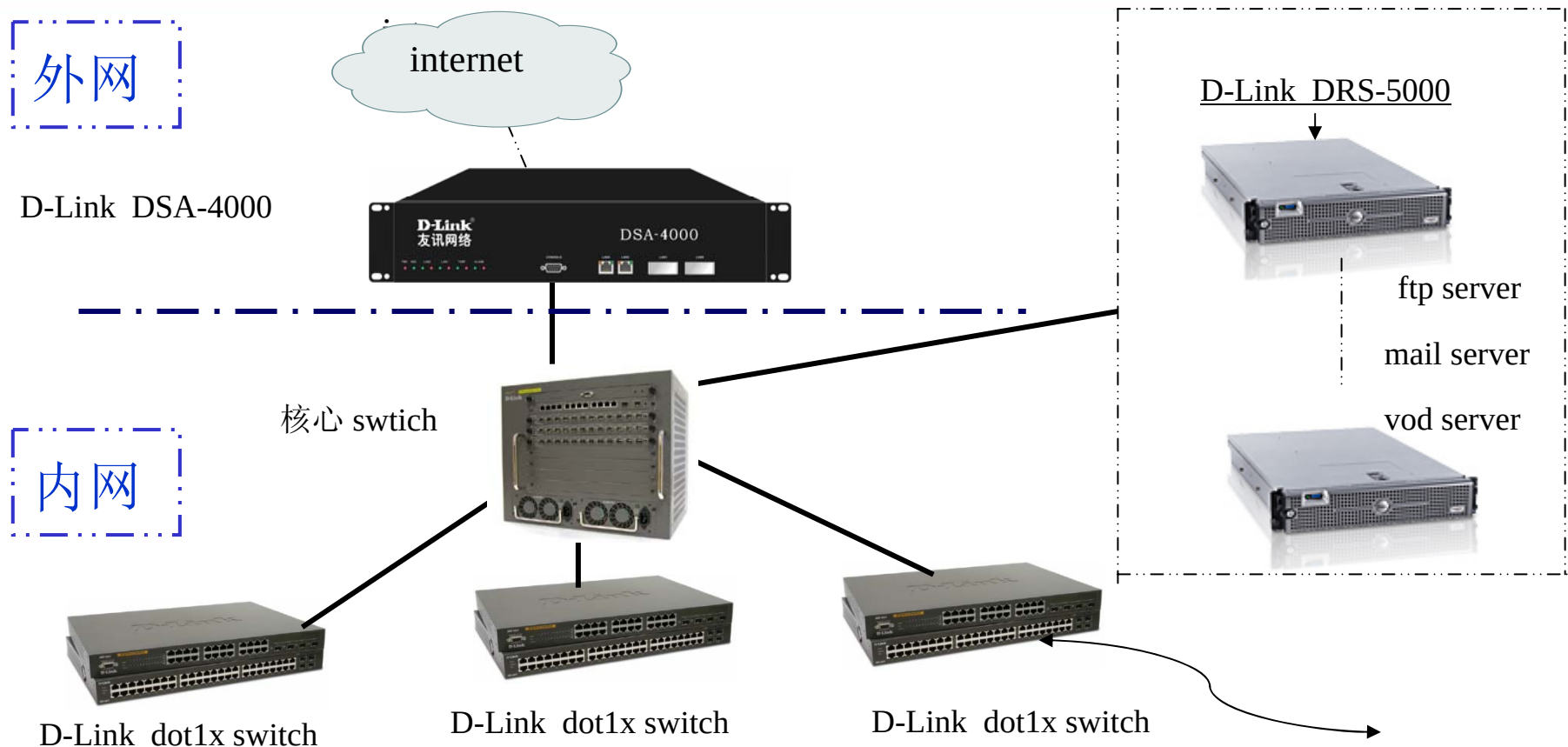
综合流控

对不同出口的流量分别进行影响有局限性

功能拓展



三、全面、丰富的认证计费计费手段



D-Link 独创的二次认证解决，接入层可采用D-Link或其它厂商支持dot1x的switch，DSA-4000高可靠性接入网关位于网络出口部分并结合后台D-Link DRS-5000认证计费运营平台，实现一次拨号二次认证方案，用户可采用此方案针对内网资源免费，上外部网络收费的策略

优点

- 1、专用客户端防止私接和代理
- 2、能融合现有所有支持802.1x的交换机，避免垄断
- 3、可定义时长、流量等多种计费策略
- 4、和现有一卡通系统完美结合，实现计费、收费人性化
化管理
- 5、锁定用户的上网地点 实现一个帐号全网漫游

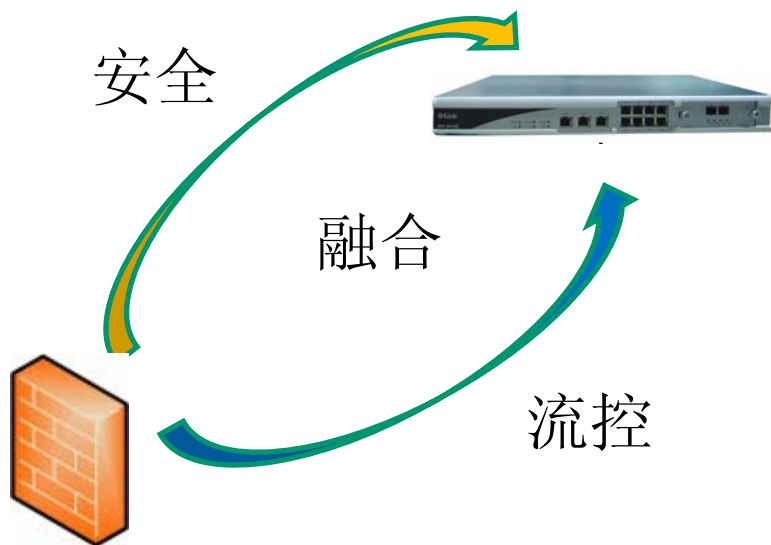
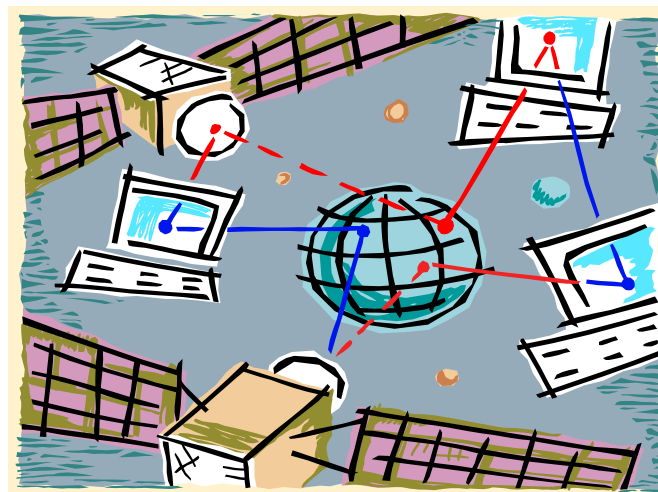
总结

- 1、流量控制的目的不在于限制，而在与疏导。把握网络中不同时段、用户、应用的分布趋势，合理疏导流量，才能真正缓解带宽和应用间的矛盾。
- 2、内网安全问题用户终端解决，真正实现内部网络的安宁
- 3、加强认真计费系统健壮性、灵活性和可扩展性，更好的为网络运营服务
- 4、网络设备的功能融合是必然趋势，毕竟单一功能的设备越多，可能的瓶颈也越多。强壮的硬件架构是融合的保障

我们的目标

通过全能流控设备、认证计费系统、智能接入交换机
完成校园网的可持续化良性运营的改造

让有限的带宽发挥更大的作用
让我们的网络环境更舒适、更安全





休息&讨论！