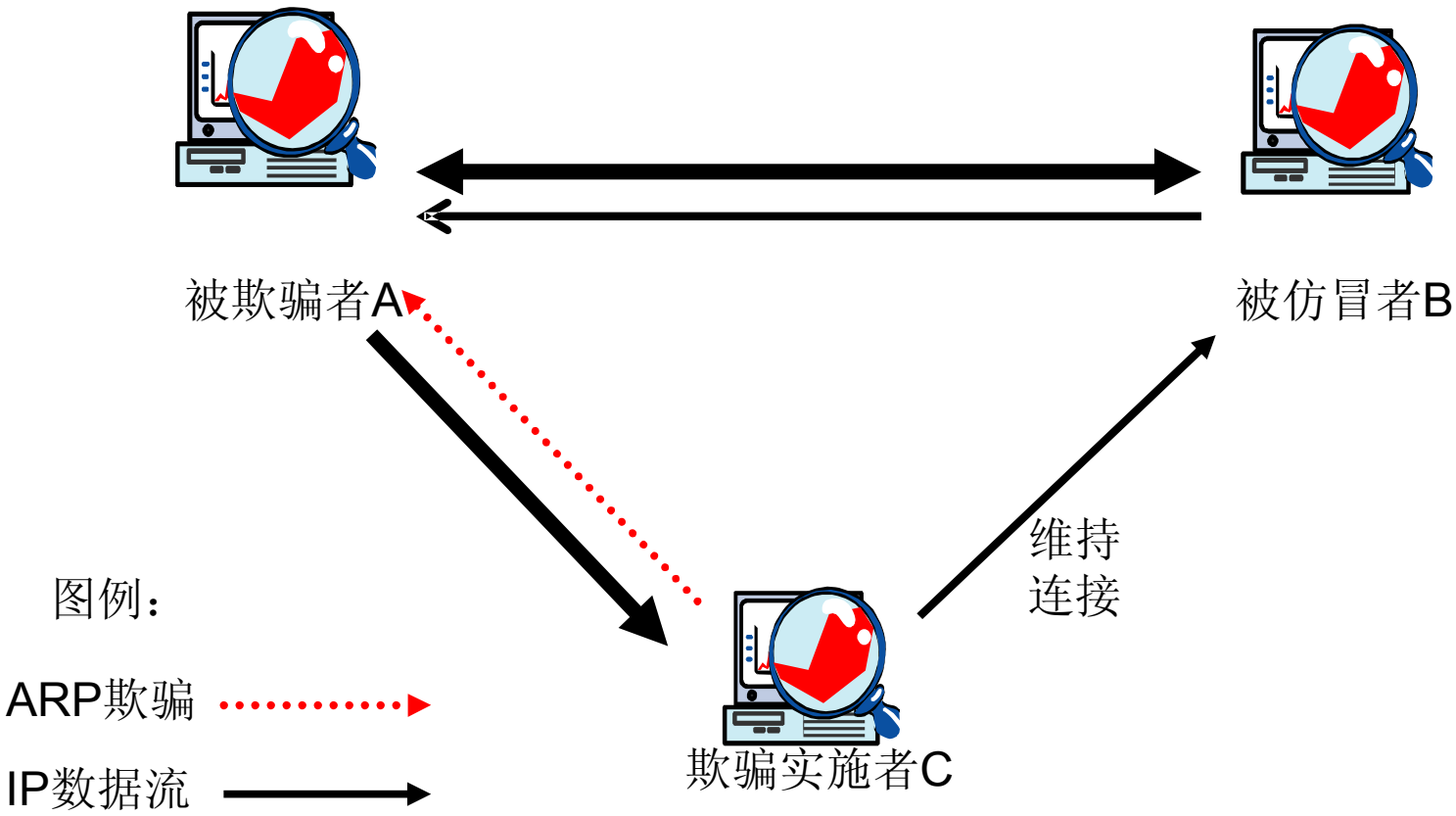
上海交通大學
Shanghai Jiao Tong Univer...

ARP欺骗校内防治讨论

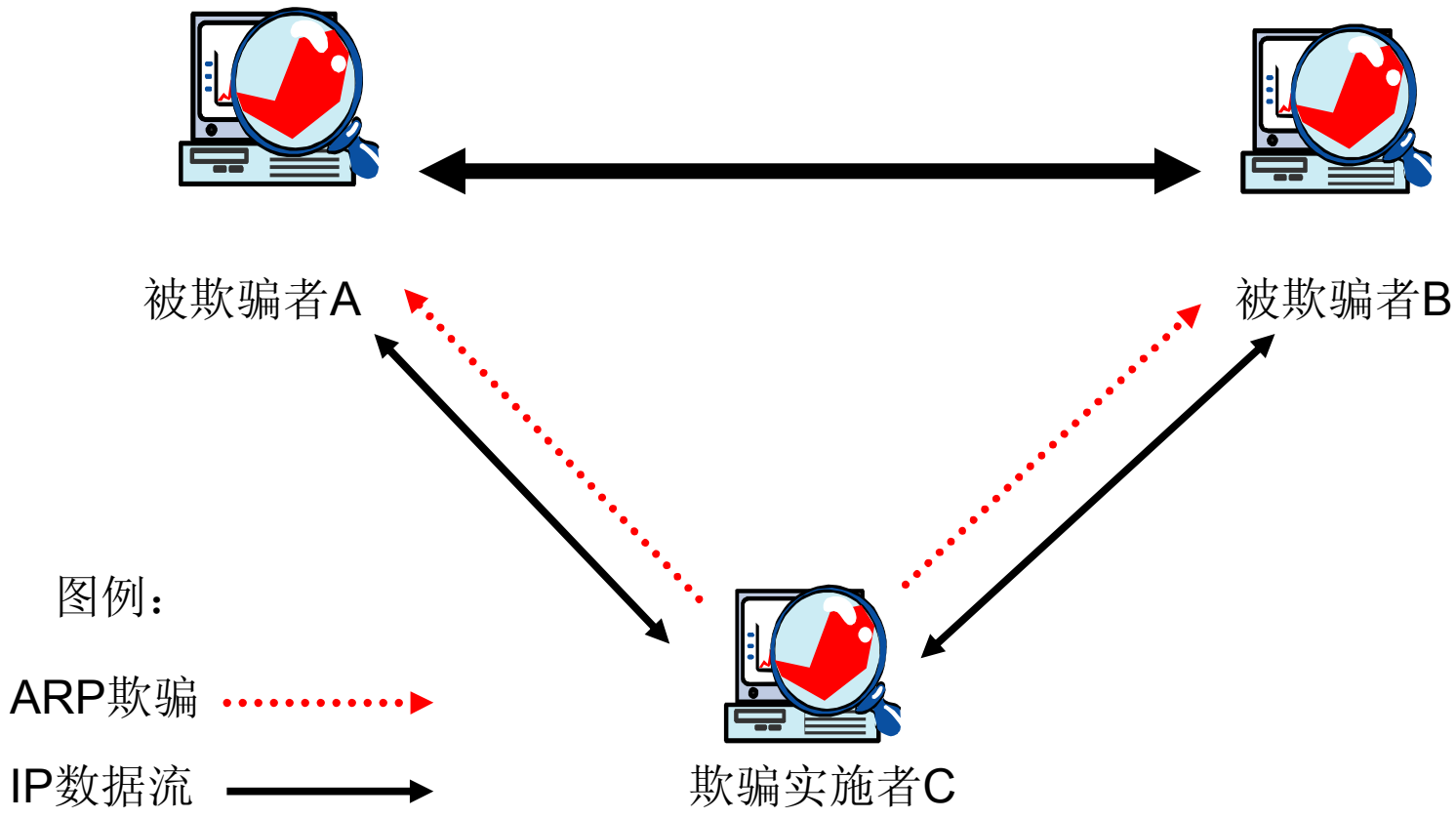
2008年4月1日

赖学亮

3.2.1 ARP单向欺骗过程图示



3.3 ARP双向欺骗过程图示



5.现有设备ARP防治措施与问题

- 1.三层架构
  - 1.两层交换机(不带ACL)
  - 2.两层半交换机(带ACL)
  - 3.三层交换机
- 2.用户隔离架构
  - 3Tnet试验网
- 3.无线设备：
  - AP与中心控制器

上海交大目前的IP地址管理方式

- 有线网全静态IP地址分配
  - 用户提交网卡地址，网络中心将该地址配如交换机端口
  - 全部分配公众网IP地址
- 无线网动态IP地址分配
  - 通过用户网关认证用户名、密码
  - 全部分配公众网IP地址

5.1.1 纯两层交换机

- 现有防治ARP欺骗措施：
  - 无。
    - 在端口绑定网卡地址，对报文MAC源地址做限制
    - 该措施对不伪造源MAC的ARP欺骗没有效果。
- 改进方向：
  - 配置端口隔离，802.1q或PVLAN，配合用户接入控制设备使用

5.1.1(续) 校两层交换机的特性

- 实达S2026G/S1926G+、S1924F+

  配置端口隔离、其中G+与F+的默认端口隔离需要使用PortVLAN模式，使用Tag VLAN模式的端口隔离的稳定性未知。曾有G+配置3个用户VLAN，一个VLAN的用户常报不通；换S2026后也没有改善(v1.7)；现换为S2126G。

- Cisco1924

  不支持广播的端口隔离，只能限制某个绑定MAC（单播目标地址）的许可源交换端口；可以配置Cisco ISL VLAN

- Cisco2924

  支持端口隔离和VLAN，支持ISL/802.1q VLAN间转换

- Bitway

  未找到端口隔离指令，支持VLAN，但现有百兆模块在引用802.1q时不能正确处理全长报文(1500)多出的4个字节

5.1.2 两层半交换机

- 现有防ARP欺骗措施：
  - 开启全局ARP检查功能
  - 在端口绑定MAC及IP信息，或只绑定IP信息

- 缺点：
  - 部分设备配置绑定的接口不能同时配置ACL
  - IP/ARP检查规则意外影响IPv6 Native应用

- 改进方向：
  - 配置端口隔离：802.1q或PVLAN，配合上层用户接入控制设备，接入端口改配速率限制策略。
  - 配置DHCP relay，支持动态绑定。

5.1.2(续) 校两层半交换机的特点

- 神州数码DCS-3926S

  am命令支持ARP防护，许可IP和IP/MAC；由于之前配置按portsecurity写，尚未启用am功能。

- 锐捷S2126G

  port-security arp-check命令开启全局ARP检查

  anti-ARP-Spoofing端口级防止单IP被欺骗

- H3C S3026C

  未发现ARP相关配置语句。

注：以上设备都支持端口隔离(PVLAN)和802.1q

5.1.3 三层交换机

- 现有防治ARP欺骗措施：
  - snmp检查设备ARP 表，对问题MAC实施二层端口封禁；
  - 静态ARP绑定，对未开放IP设置为黑洞；
  - 根据DHCP结果检查ARP表合法性
- 缺点：
  - 部分交换机的静态ARP条目有上限，
  - 只能检测针对网关的欺骗。
  - 部分设备不支持同端口内的ARP Proxy。
  - 3层交换机默认不检查用户源IP/MAC，用户流量不记账
- 改进方向：
  - 将有问题的用户隔离到杀毒的VLAN，避免对其他用户的影响
  - 功能较弱的交换机：降为2层汇聚设备，配置端口隔离、802.1q或PVLAN，汇聚到用户接入设备。
  - 功能较强的交换机：缩小网段划分，减少ARP欺骗的影响范围，使用私有地址的情况下可以给每个用户端口配置独立的VLAN网关

5.1.3(续) 校三层交换机的特性

- Extreme 24

  支持PVLAN端口隔离、但不能启用同端口ARP Proxy响应

- Extreme ***i系列

  比不带i系列更支持同端口ARP Proxy响应；支持基于DHCP绑定ARP

- 锐捷S3550-24

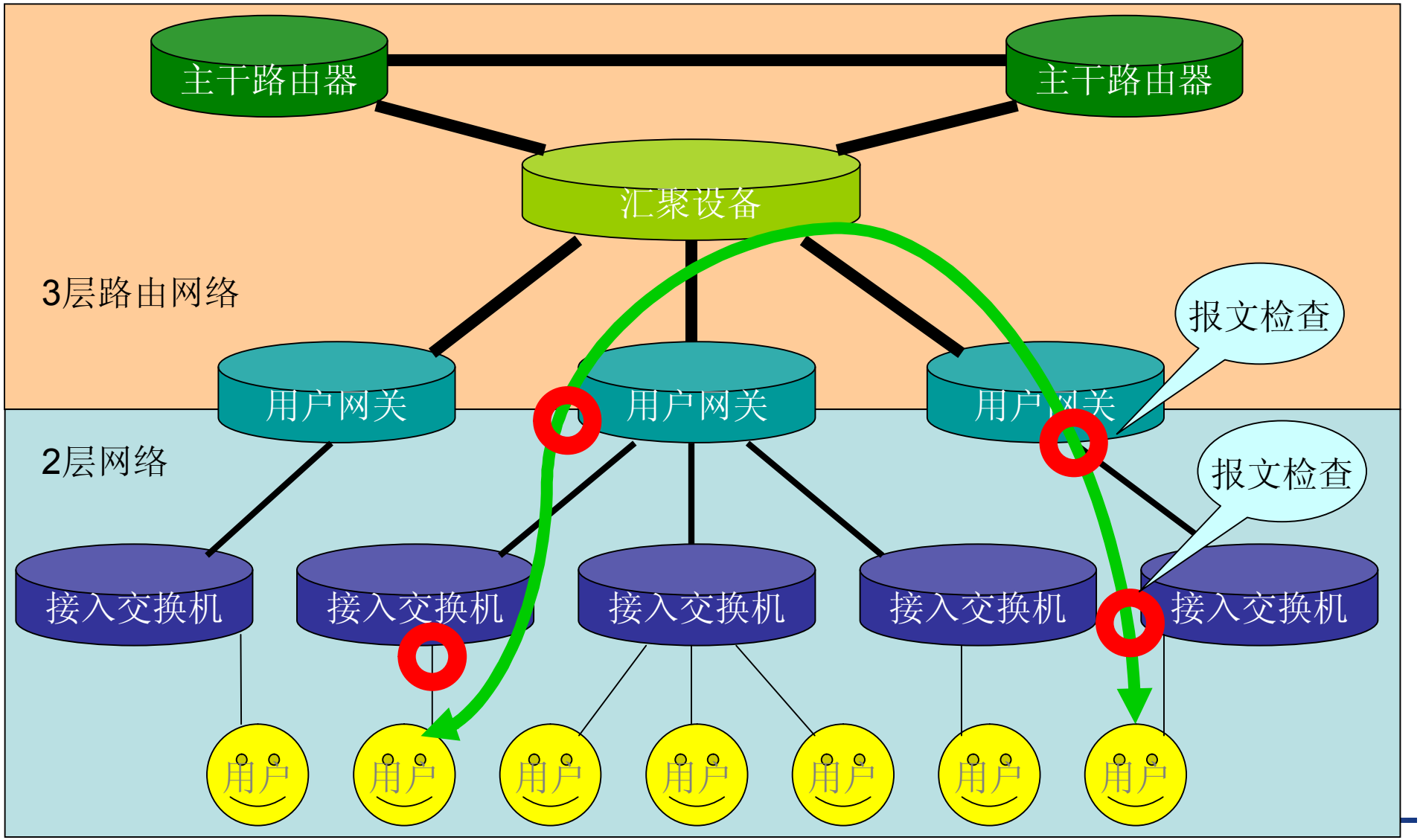
  通过switchport protected设置端口隔离

- 神州数码5950

  指令防止arp被更新、动态arp转静态；通过private VLAN的形式支持端口隔离。

5.1.4 三层路由架构图示

比较隔离架构



5.2.1 用户隔离+用户接入设备架构

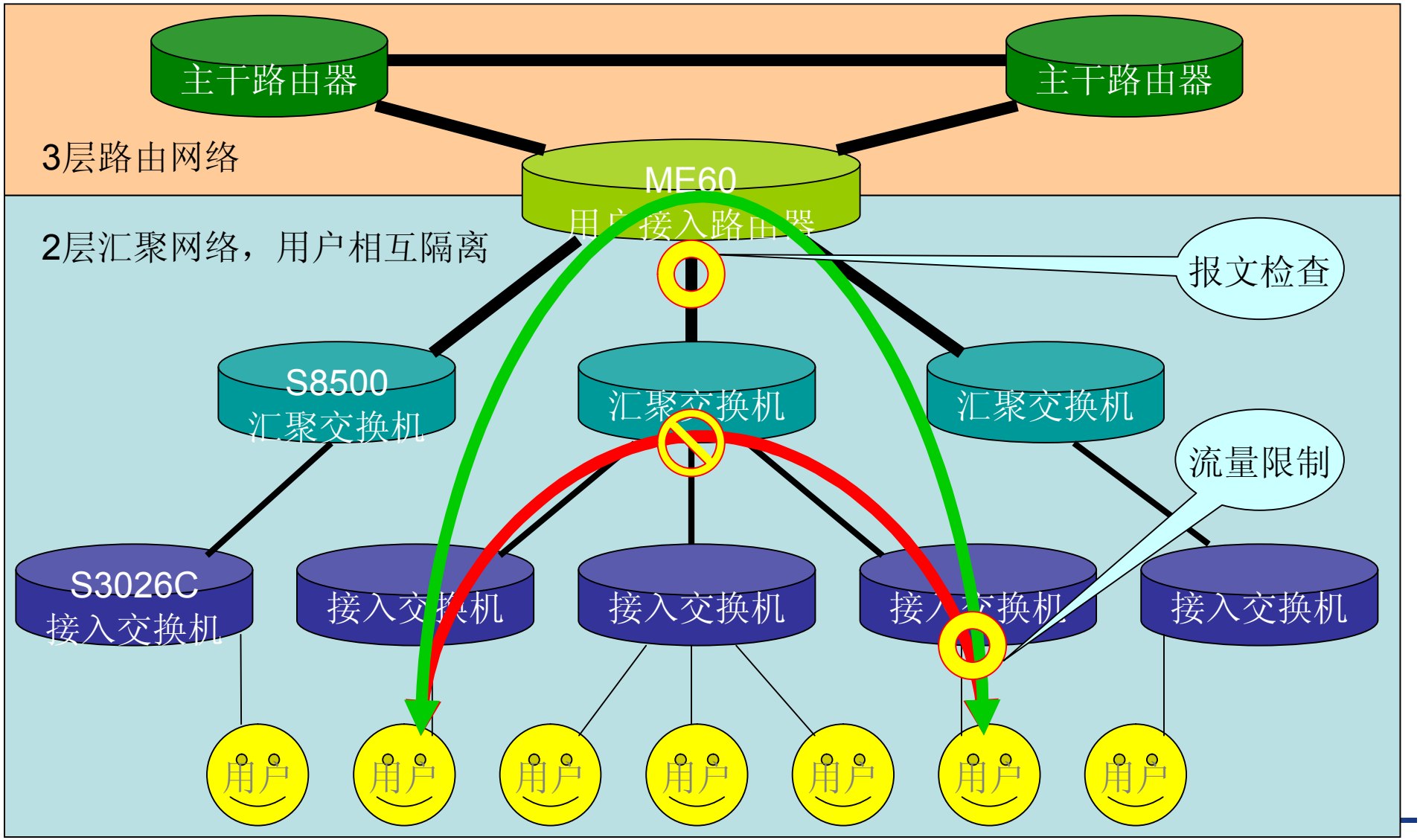
- 接入交换机：
  - 用户接口带宽限制；用户间PVLAN或VLAN隔离；
- 汇聚交换机：
  - 流量汇聚，PVLAN保持隔离、802.1q VLAN汇聚上行。
- 用户接入路由器：
  - 检查上行报文源IP、源MAC、帐号、VLAN等信息；
  - 不采信用户的ARP更新；
  - 弹出Portal页面与计费等。
- ARP欺骗防治：
  - 用户隔离，网关稳定；ARP欺骗不影响通讯。
  - ARP报文可能大量消耗接入路由器的CPU。
- 缺点：
  - 价格较高；可靠性保证不如3层架构灵活

5.2.2 用户隔离实例 3Tnet实验网

- 核心：
  - 华为ME-60多用途路由器，
  - 10G单板联S8500，每个接口拥有独立的4094个VLAN号。
- 汇聚：
  - H3C Quidway S8500汇聚交换机
  - 三层交换机但仅做二层转发，
  - 10Gx1 + 1Gx24x4
- 接入：
  - H3C Quidway S3026C 用户接入交换机
  - 100Mx24 + 1G x 1
  - 每个百兆用户端口分配独立的802.1q VLAN号
  - 1G接口汇聚24+1个VLAN上行，保证用户相互隔离。

5.2.3 隔离架构图示

比较路由架构

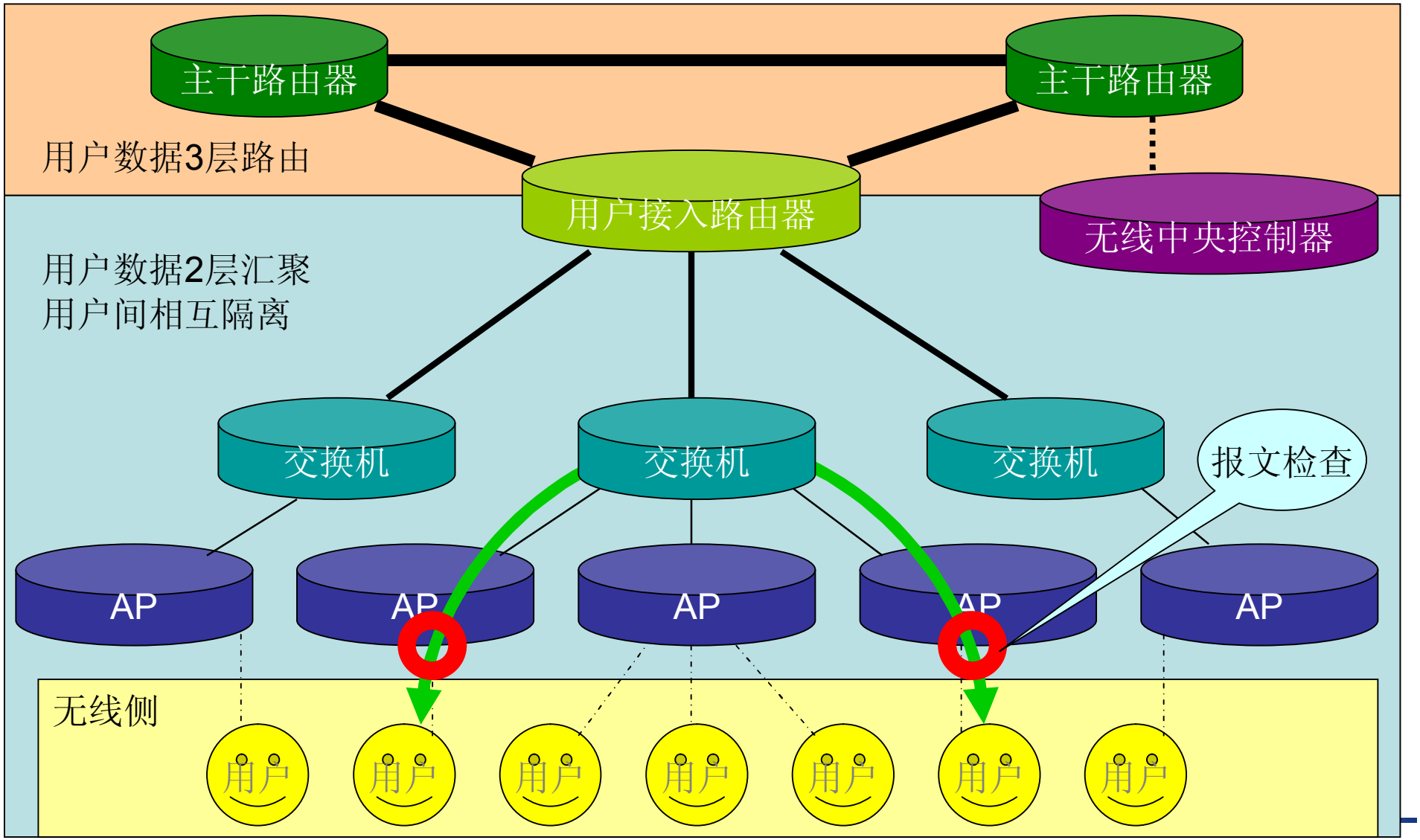


5.3.1 无线架构 隔离与否的取舍

- 用户间相互隔离的特性
  - 防止无谓的组播占用珍贵的无线带宽
  - 防止用户间的干扰
  - 但流量集中，无线测交换应用为主时主干网带宽浪费严重。
  - 对控制器要求高，控制器是单点故障，
- 非隔离架构则必须在无线访问点(AP)侧阻隔所有的已知用户干扰，包括
  - TCP/IP的DNS,DHCP干扰
  - IPv6的RA广播公告
  - PPPoE的服务器应答
  - ARP的本地网关IP地址应答
  - 抑制过量广播
- 非隔离架构的AP最好能够实现DHCP relay和DHCP自动binding，确保源地址可信。

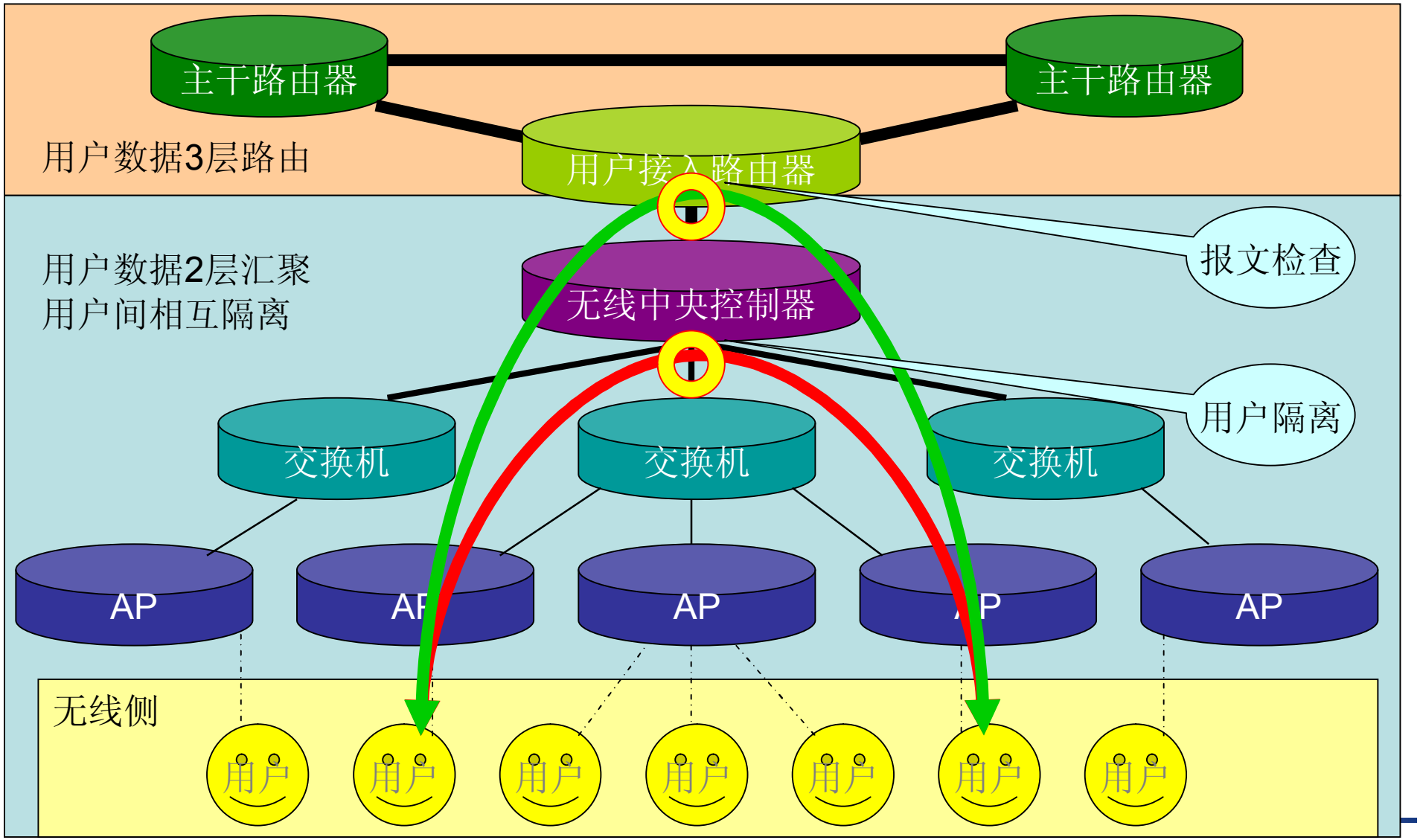
5.3.2 无线开放架构图示

比较隔离架构



5.3.3 隔离架构图示

比较开放架构



5.3.4 Cisco胖AP的防ARP的ACL

- access-list 1103 permit 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000 ffff.ffff.ffff 0xC 2 eq 0x800 //放行所有IP报文
- access-list 1103 deny 0000.0000.0000 ffff.ffff.ffff 3333.0000.0001 0000.0000.0000 0xC 2 eq 0x86DD //禁止IPv6全站点路由公告
- access-list 1103 permit 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000 ffff.ffff.ffff 0xC 2 eq 0x86DD //放行所有IPv6报文
- access-list 1103 deny 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000 ffff.ffff.ffff 0x1C 4 eq 0xD3505101// 禁止ARP声称211.80.81.1网关
  // 由于ACL写法限制，本条不止针对ARP报文，而是针对所有报文
- access-list 1103 permit 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000 ffff.ffff.ffff 0xC 2 eq 0x806 // 放行其他ARP报文
- 以上的写法并不能限制用户手工指定IP地址，也不能防止发往网关的欺骗报文。

5.3.5 无线用户网关chillispot

- 优点
  - 基于用户态tun/tap接口，UNIX系统间迁移方便。
  - 自维护IP-ARP表，不受ARP欺骗影响
  - 自维护DHCP列表，对不在列表中的地址不会做ARP广播问询(节省无线广播包开销)
  - 弹出Web Portal窗口，统计用户流量
- 不足
  - 用户态程序效率不如系统态，
  - 暂不支持IPv6，
  - 不能识别配错IP、配错代理服务器的用户

5.3.6 校无线网络设备

- Cisco 胖AP及汇聚层网络
  - AP未配置用户隔离，汇聚层也未配置隔离
  - AP上配置ACL防止冒充网关，但网关本身仍可能会被欺骗
- Symbol 瘦AP及中控WS5100
  - 中控不能启路由，只能做桥接。
  - 中控支持用户隔离，但不支持ARP相关ACL。
- 用户接入网关
  - 昂科AC：不能防范ARP欺骗
  - 三层交换机：没有用户认证功能，配合DHCP可以部分防范ARP欺骗(结合ACL，可能不适用与互联口)；但没有记账功能。
  - Chillispot及相关免费AC：完全防止ARP欺骗，配合瘦AP做用户隔离后隔离用户间不互通(查chilli原版代码，非实验结果)，用户认证、DHCP分配时fork进程占用CPU较高，影响正常流量
  - 华为ME-60路由器：根据说明书，可以很好的完成接入网关的功能，也有3Tnet的稳定性保证。但由于属于试验网设备，不能轻易更改配置和接线。

6. 用户端口隔离的优缺点

- 隔离措施的分类
- 隔离的优点
- 隔离的问题

6.1 隔离措施的分类

- **端口隔离**是解决傻2层设备间用户互相干扰的好办法，一般有PVLAN隔离与VLAN隔离
  - PVLAN隔离：在同一个2层VLAN内人为设置端口间不能互通。一般适用PPPoE网络。无线交换机的用户隔离也类似于此。
    优点：设备要求不高，Extreme-i也可以对同端口ARP Proxy提供较好的支持。
    缺点：是一般3层设备对同一个物理端口下的VLAN个数有上限，主要是多播复制上限。
  - 802.1q VLAN隔离：每用户端口独立VLAN
    优点：用户来源可追溯到端口，底层端口可控，安全性更好
    缺点：对设备要求高，硬件投资昂贵。

6.2 隔离的优点

- 用户间互不干扰，
- 底层通讯协议的漏洞得以绕过(ARP/PPPoE/IPv6 ND)，
- 网络服务层次结构鲜明，权责明确，便于查找故障。

6.2 隔离的问题

- 用户间2层互不相通，无法以太帧通讯，破坏了以太网平面网的假设特性
- 用户通过3层协议绕转通讯重复占用汇聚链路带宽、造成延时（语音通讯等）
- 需要对平面网重新规划，2层、3层设备要重配置，不支持必要功能的设备要重购置
- 待补充

完毕

- 谢谢
- 意见建议请联系 colins@sjtu.edu.cn
- 最后修改：2008年5月26日10时57分