**华中师大一附中校园局域网环境下**

**若干安全问题及对策**

撰写人：叶凯

2014.11.13

**目录**

[一、前言 3](#_Toc403654244)

[二、校园网安全问题的现象及危害 4](#_Toc403654245)

[（一）ARP攻击现象及危害 4](#_Toc403654246)

[1、故障现象 4](#_Toc403654247)

[2、故障危害 5](#_Toc403654248)

[（二）DHCP现象及危害 5](#_Toc403654249)

[1、故障现象 5](#_Toc403654250)

[2、故障危害 6](#_Toc403654251)

[（三）广播风暴现象及危害 6](#_Toc403654252)

[1、故障现象 6](#_Toc403654253)

[2、故障危害 6](#_Toc403654254)

[三、校园网病毒攻击原理 7](#_Toc403654255)

[（一）ARP攻击原理 7](#_Toc403654256)

[（二）DHCP攻击原理 9](#_Toc403654257)

[（三）广播风暴攻击原理 11](#_Toc403654258)

[四、校园网安全应对措施 14](#_Toc403654259)

[（一）ARP攻击应对措施 14](#_Toc403654260)

[（二）DHCP攻击应对措施 16](#_Toc403654261)

[（三）广播风暴应对措施 17](#_Toc403654262)

[五、结语 18](#_Toc403654263)

# 一、前言

二十一世纪以来，随着互联网和计算机网络技术在我国的发展和普及，全国各地的中小学都逐步建立起自己的校园网。中小学通过校园网实现基本的上网功能之外，还能管理和维护学校网站并发布学校的通知和新闻，另外可以对学生的选课、学籍以及考试成绩等方面进行管理，同时还有诸如数字图书馆等多方面的内容，可以说校园网在中小学的日常管理中有着不可替代的作用，校园网的出现使得学校的各方面的管理都变得更加地数字化。除此之外，校园网的运用，不但可以提高课堂教学效率，又能丰富学生的文化知识视野，网络与信息系统的应用已经成为中小学学校管理和学生学习必不可少的帮手。因此，校园网作为学校信息化建设的基础设施，它是学校实现信息化的一个重要平台，并在教学支持服务、教学教务管理、行政管理和校内外信息沟通等方面起着举足轻重的作用。

华中师大一附中作为全国知名学校，聚集了优秀的教师资力量，具备了完善的管理体制。校园网自建设以来就为学校的管理和学生的学习提供着非常关键的支持。但是随着网络应用的不断加深，校园网在给中小学带来便利的同时，网络的安全问题也不断暴露出来，校园网中存在的问题也频频发生，网络入侵、垃圾邮件、数据泄漏等问题也时有发生，这给已经习惯利用校园网的中小学带来了许多的麻烦。这些问题的发生也不但给校园的日常管理活动带来了影响，同时数据泄漏等问题更是让广大师生感到自己的安全受到了威胁。

因此，为了让校园网更好的发挥其作用，就必须要解决校园网的安全问题。如何保障网络的正常运行、资源的合法访问，使网络免受黑客、病毒、恶意软件和其他不良意图的攻击就显得尤为重要。本文通过对华中师大一附中校园网中出现的各种问题进行分析，从中发现网络中存在的各种潜在威胁，针对校园网中影响校园网络安全和性能的ARP Snooping 、DHCP Snooping 、广播风暴等网络病毒进行观察、分析和模拟实验，掌握每种病毒的发生状况、带来的威胁以及如何通过技术手段有针对性的解决这些网络病毒，对日后的校园网的网络问题的解决具有一定的借鉴意义。

# 二、校园网安全问题的现象及危害

就目前而言，无论是在局域网还是在广域网中，都存在着自然或者人为等诸多因素造成的潜在威胁，校园网也因此而面临着各种安全问题。我校目前的网络情况虽说基本稳定，但在局部区域仍然存在着不同的网络攻击。因此，及时发现和解决这些潜在的威胁，保证网络的安全和通畅就显得尤为重要。针对华中师大一附中网络安全和性能分析，影响校园网安全问题主要表现在以下三个方面：

## （一）ARP攻击现象及危害

### 1、故障现象

实例：在2号教学楼发现有部分老师无法正常的使用网络上网，网络断断续续。笔者在PING网关的时候发现网络掉包，延时不大，时断时续。而且在上网的高峰时会出现，当用户较少的时候没有此现象。与此同时，在校园网的其他网段中，没有用户出现掉网的现象，说明此种现象只是针对同一网段的用户（即在同一VLAN中产生影响）。

经过相关故障检查和资料查找，该故障可能是由于ARP攻击造成的。ARP欺骗木马的中毒现象表现为：使用局域网时会突然掉线，过一段时间后又会恢复正常。例如客户端状态频频变红，用户频繁断网，IE浏览器频繁出错，以及一些常用软件出现故障等。如果局域网中是通过身份认证上网的，会突然出现可认证，但不能上网的现象（无法ping通网关），重启机器或在MS-DOS窗口下运行命令arp-d后，又可恢复上网。

ARP欺骗木马只需成功感染一台电脑，就可能导致整个局域网都无法上网，严重的甚至可能带来整个网络的瘫痪。该木马发作时除了会导致同一局域网内的其他用户上网出现时断时续的现象外，还会窃取用户密码。如盗取QQ密码、盗取各种网络游戏密码和账号去做金钱交易，盗窃网上银行账号来做非法交易活动等，这是木马的惯用伎俩，给用户造成了很大的不便和巨大的经济损失。

基于ARP协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的ARP数据包，数据包内包含有与当前设备重复的Mac地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。一般情况下，受到ARP攻击的计算机会出现两种现象：（1）不断弹出“本机的0-255段硬件地址与网络中的0-255段地址冲突”的对话框。（2）计算机不能正常上网，出现网络中断的症状。因为这种攻击是利用ARP请求报文进行“欺骗”的，所以防火墙会误以为是正常的请求数据包，不予拦截。因此普通的防火墙很难抵挡这种攻击。

### 2、故障危害

ARP攻击的危害主要有两个方面：从ARP攻击的原理来看，这种攻击使得受害主机的所有网络数据都将通过攻击者进行转发，这样一来，要窃取信息或控制流量就变得轻而易举；另一方面，由于ARP缓存会不断刷新，有的时候真正的网关会偶尔“清醒”，当真正的网关参与到数据包转发中来时，由于做了一个切换动作，可能会有频繁的短暂掉线现象。所以，如果Web服务器所在网络中发生了ARP攻击，将导致Web服务器不可访问。

## （二）DHCP现象及危害

**1、故障现象**

实例：在2号教学楼有老师反映自己的电脑接上网线之后无法上网，在经过提示修复本地网络连接之后可以正常使用，但下午又出现无法上网的情况。笔者到故障点检查本地网络连接，发现所获取的IP地址为192.168.1.X ，不是我校合法的IP地址（我校合法IP为10.2.X.X）。而且除了本网段的电脑之外，其他网段的电脑没有出现这个问题。

我们对周边办公室进行查看，找到一台TP-LINK无线路由器。从学校接入层交换机接出的网线正好接在无线路由器的WAN口上，而且无线路由器本身就自带DHCP功能，可以自己下发IP地址。故障电脑所获取的IP地址也和无线路由器自身下发的IP地址段重合。因此判断无法上网的老师的电脑获取的地址是从最近的TP-LINK无线路由器上获取的，而不是从我校的DHCP服务器获取。

### 2、故障危害

DHCP攻击会产生大量的DHCP报文，在将这些报文传送给服务器。这样一方面会恶意的耗尽IP资源，使得合法的用户无法获得IP；另一方面，如果交换机开启了DHCP SNOOPING功能，会将大量的DHCP报文传给服务器，使得DHCP服务器始终处于高运转，最终导致服务器瘫痪。

## （三）广播风暴现象及危害

### 1、故障现象

实例：学校行政楼二层的老师反映网络有问题，网络时断时续。笔者在第一时间赶到事发地点，在二层某一办公室的电脑上利用“ping 10.2.0.1 –t”命令测试网络通断，命令中的 IP 地址是核心交换机地址，网络果然时通时断，并且延时很大。一段时间后停止测试，命令返回的结果显示数据“lost=45%”，随机到二楼其它办公室用同样命令测试网络，结果一样。45% 的大面积数据丢包率说明该网络已经不能正常使用。

经过相关故障检查和资料查找，该故障可能是由于广播风暴引起的。当广播数据充斥网络无法处理，并占用大量网络带宽，导致正常业务不能运行，甚至彻底瘫痪，这就发生了“广播风暴”。一个数据帧或包被传输到本地网段（由广播域定义）上的每个节点就是广播；由于网络拓扑的设计和连接问题，或其他原因导致广播在网段内大量复制，传播数据帧，导致网络性能下降，甚至网络瘫痪，这就是广播风暴。一般情况下，受到广播风暴影响的计算机会出现以下现象：网络堵塞，网速慢，严重时会导致网络中断。

### 2、故障危害

广播风暴现象是最常见的数据洪泛(flood）之一，是一种典型的雪球效应。当广播风暴产生时，以太介质几乎充满广播数据包，网络设备接口上统计的报文速率达到106数量级，设备处理器高负荷运转。不仅网络设备会受到影响，而且所有的主机都要接收链路层的广播数据包，因而受到危害。每秒数万级的数据包通常都会使网卡工作异常繁忙，操作系统反映迟缓，网络通讯严重受阻，严重地危害了网络的正常运行。

# 三、校园网病毒攻击原理

针对我校的校园网安全问题中出现地ARP Snooping 、DHCP Snooping 、广播风暴等故障问题，在如何解决这些问题之前，我们应该分析它们的攻击原理，才能为更好的提出解决措施做好准备。

## （一）ARP攻击原理

ARP攻击就是通过伪造IP地址和MAC地址实现ARP欺骗，能够在网络中产生大量的ARP通信量使网络阻塞，攻击者只要持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击。

ARP攻击主要是存在于局域网网络中（局域网络的同一网段中，对跨网段用户没有影响），局域网中若有一个人感染ARP木马，则感染该ARP木马的系统将会试图通过“ARP欺骗”手段截获所在网络内其它计算机的通信信息，并因此造成网内其它计算机的通信故障。

要了解故障原理，我们先来了解一下ARP协议。

在局域网中，通过ARP协议来完成IP地址转换为第二层物理地址（即MAC地址）的。ARP协议对网络安全具有重要的意义。通过伪造IP地址和MAC地址实现ARP欺骗，能够在网络中产生大量的ARP通信量使网络阻塞。

ARP协议是“Address Resolution Protocol”（地址解析协议）的缩写。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的MAC地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址，而目标MAC地址是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。

每台安装有TCP/IP协议的电脑里都有一个ARP缓存表，表里的IP地址与MAC地址是一一对应的，例如下表所示。

主机 IP地址 MAC地址

A 192.168.2.1 aa-aa-aa-aa-aa-aa

B 192.168.2.2 bb-bb-bb-bb-bb-bb

C 192.168.2.3 cc-cc-cc-cc-cc-cc

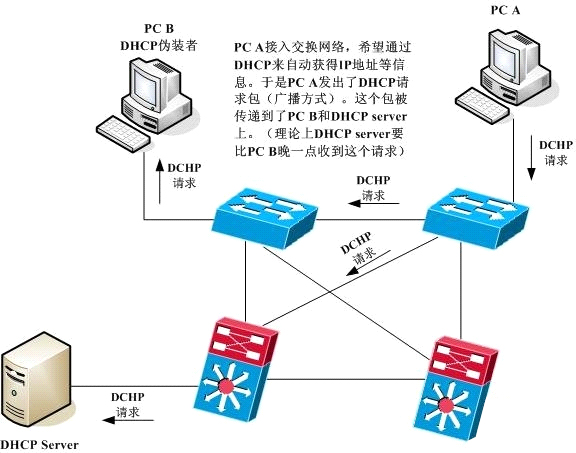
D 192.168.2.4 dd-dd-dd-dd-dd-dd

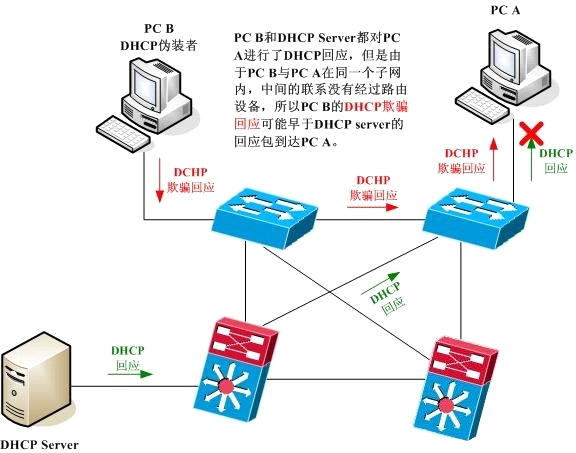
我们以主机A（192.168.2.1）向主机B（192.168.2.2）发送数据为例。当发送数据时，主机A会在自己的ARP缓存表中寻找是否有目标IP地址。如果找到则知道目标MAC地址，直接把目标MAC地址写入帧里面即可发送；如果在ARP缓存表中没有找到相对应的IP地址，主机A就会在网络上发送一个广播，目标MAC地址是“ff-ff-ff-ff-ff-ff”，这表示向同一网段内的所有主机发出这样的询问：“192.168.2.2的MAC地址是什么？”网络上其他主机并不响应ARP询问，只有主机B接收到这个帧时，才向主机A做出这样的回应：“192.168.2.2的MAC地址是bb-bb-bb-bb-bb-bb”。这样主机A就知道主机B的MAC地址，它就可以向主机B发送信息。同时它还更新了自己的ARP缓存表，下次再向主机B发送信息时，直接从ARP缓存表里查找即可。ARP缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除，这样可以大大减少ARP缓存表的长度，加快查询速度。

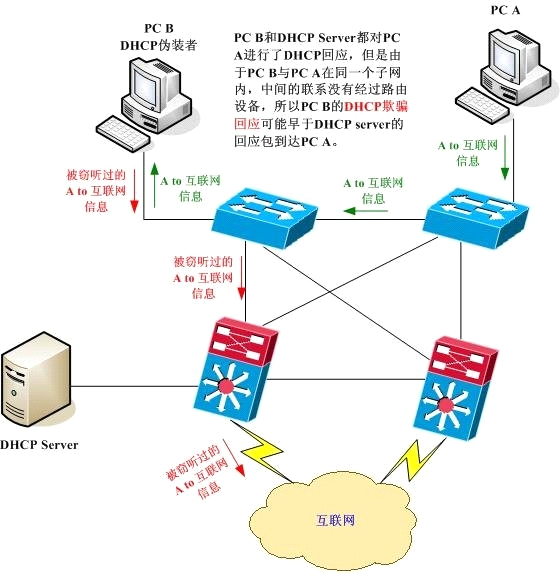
从上面可以看出，ARP协议的基础就是信任局域网内所有的人，那么就很容易实现在以太网上的ARP欺骗。对目标A进行欺骗，A去Ping主机C却发送到了dd-dd-dd-dd-dd-dd这个地址上。如果进行欺骗的时候，把C的MAC地址骗为dd-dd-dd-dd-dd-dd，于是A发送到C上的数据包都变成发送给D的了。正好是D能够接收到A发送的数据包，说明嗅探成功。但是A对这个变化一点都没有意识到，但是接下来的事情就让A产生了怀疑。因为A和C连接不上了。D对接收到A发送给C的数据包可没有转交给C。接下来做“man in the middle”，进行ARP重定向。打开D的IP转发功能，A发送过来的数据包，转发给C，好比一个路由器一样。不过，假如D发送ICMP重定向的话就中断了整个计划。D直接进行整个包的修改转发，捕获到A发送给C的数据包，全部进行修改后再转发给C，而C接收到的数据包完全认为是从A发送来的。不过，C发送的数据包又直接传递给A，倘若再次进行对C的ARP欺骗。现在D就完全成为A与C的中间桥梁了，对于A和C之间的通讯即可了如指掌。

## （二）DHCP攻击原理

以下图解能很直观的解释出DHCP攻击的原因。







DHCP攻击就是从最近的DHCP服务器拿地址，当攻击者伪装成DHCP服务器向用户发送DHCP返回的报文时，用户就会拿到错误的地址，导致网络解析错误而无法上网。

## （三）广播风暴攻击原理

要想正确理解广播风暴的原理，我们必须了解一下工作在网络中的网络设备的工作原理。目前，华中师大一附中基本上都是交换连接网络。我们首先来了解一下一些基本知识：

（1）交换机的定义：交换机是一种基于MAC(网卡的硬件地址)识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

现在，交换机已经替代了我们原来比较熟悉的网络设备集线器，又称Hub。但是这并不意味着，我们不需要了解Hub的基本知识。

（2）集线器的定义：集线器(Hub)属于数据通信系统中的基础设备，它和双绞线等传输介质一样，是一种不需任何软件支持或只需很少管理软件管理的硬件设备，它被广泛应用到各种场合。集线器工作在局域网(LAN)环境，像网卡一样，应用于OSI参考模型第一层，因此又被称为物理层设备。集线器内部采用了电器互联，当维护LAN的环境是逻辑总线或环型结构时，完全可以用集线器建立一个物理上的星型或树型网络结构。在这方面，集线器所起的作用相当于多端口的中继器。其实，集线器实际上就是中继器的一种，其区别仅在于集线器能够提供更多的端口服务，所以集线器又叫多口中继器。

（3）交换机与集线器的区别

现在，我们经常会存在这样一个技术误区，我们用的是交换机，数据全部是点对点转发的，为什么还会产生广播风暴呢?我们在充分了解了交换机与集线器的功能区别后，就会明白，使用交换机作为网络设备的网络，为什么会出现广播风暴。

交换机与集线器的本质区别：用集线器组成的网络称为共享式网络，而用交换机组成的网络称为交换式网络。共享式以太网存在的主要问题是所有用户共享带宽，每个用户的实际可用带宽随网络用户数的增加而递减。这是因为当信息繁忙时，多个用户可能同时“争用”一个信道，而一个信道在某一时刻只允许一个用户占用，所以大量的用户经常处于监测等待状态，致使信号传输时产生抖动、停滞或失真，严重影响了网络的性能。

在交换式以太网中，交换机提供给每个用户专用的信息通道，除非两个源端口企图同时将信息发往同一个目的端口，否则多个源端口与目的端口之间可同时进行通信而不会发生冲突。通过实验测得，在多服务器组成的LAN中，处于半双工模式下的交换式以太网的实际最大传输速度是共享式网络的1.7倍，而工作在全双工状态下的交换式以太网的实际最大传输速度可达到共享式网络的3.8倍。交换机只是在工作方式上与集线器不同，其他的如连接方式、速度选择等与集线器基本相同，目前的交换机同样从速度上分为10M、100M和1000M几种，所提供的端口数多为8口、16口和24口几种。交换机在局域网中主要用于连接工作站、Hub、服务器或用于分散式主干网。

（4）广播风暴的原理

通过对以上网络设备的了解，我们就可以简单分析出来，网络产生广播风暴的原因了。一般情况下，产生网络广播风暴的原因，主要有以下几种：

网络设备原因：我们经常会有这样一个误区，交换机是点对点转发，不会产生广播风暴。在我们购买网络设置时，购买的交换机，通常是智能型的Hub，却被奸商作为交换机来卖。这样，在网络稍微繁忙的时候，肯定会产生广播风暴了。

网卡损坏：如果网络机器的网卡损坏，也同样会产生广播风暴。损坏的网卡，不停向交换机发送大量的数据包，产生了大量无用的数据包，产生了广播风暴。由于网卡物理损坏引起的广播风暴，故障比较难排除，由于损坏的网卡一般还能上网，我们一般借用Sniffer局域网管理软件，查看网络数据流量，来判断故障点的位置。

网络环路：曾经在一次的网络故障排除中，发现一个很可笑的错误，一条双绞线，两端插在同一个交换机的不同端口上，导致了网络性能急骤下降，打开网页都非常困难。这种故障，就是典型的网络环路。网络环路的产生，一般是由于一条物理网络线路的两端，同时接在了一台网络设备中。

网络病毒：目前，一些比较流行的网络病毒，Funlove、震荡波、RPC等病毒，一旦有机器中毒后，会立即通过网络进行传播。网络病毒的传播，就会损耗大量的网络带宽，引起网络堵塞，引起广播风暴。

黑客软件的使用：目前，一些上网者，经常利用网络执法官、网络剪刀手等黑客软件，对网吧的内部网络进行攻击，由于这些软件的使用，网络也可能会引起广播风暴。

要想做到对故障的快速判断，良好扎实的基础知识，是不可缺少的。因此大家在日后的学习中，不要忽略了对基础知识的学习!

# 四、校园网安全应对措施

在了解和分析我校校园网中出现地安全问题后，我们针对不同的网络故障提出相应的解决方案，方案如下：

## （一）ARP攻击应对措施

防止ARP攻击是比较困难的，修改协议也是不大可能。但是有一些工作是可以提高本地网络的安全性。

在电脑上：

首先，如果一个错误的记录被插入ARP或者IP route表，可以用两种方式来删除。

a. 使用arp –d host\_entry

b. 自动过期，由系统删除

这样，可以采用以下的一些方法：

（1）减少过期时间

#ndd –set /dev/arp arp\_cleanup\_interval 60000

#ndd -set /dev/ip ip\_ire\_flush\_interval 60000

60000=60000毫秒默认是300000

加快过期时间，并不能避免攻击，但是使得攻击更加困难，带来的影响是在网络中会大量的出现ARP请求和回复，请不要在繁忙的网络上使用。

（2）建立静态ARP表

这是一种很有效的方法，而且对系统影响不大。缺点是破坏了动态ARP协议。可以建立如下的文件。

test.nsfocus.com 08:00:20:ba:a1:f2

user. nsfocus.com 08:00:20:ee:de:1f

使用arp –f filename加载进去，这样的arp映射将不会过期和被新的ARP数据刷新，除非使用arp –d才能删除。但是一旦合法主机的网卡硬件地址改变，就必须手工刷新这个arp文件。这个方法，不适合于经常变动的网络环境。

（3）禁止ARP

可以通过ipconfig interface –arp 完全禁止ARP，这样，网卡不会发送ARP和接受ARP包。但是使用前提是使用静态的ARP表，如果不在apr表中的计算机，将不能通信。这个方法不适用与大多数网络环境，因为这增加了网络管理的成本。但是对小规模的安全网络来说，还是有效可行的。

在交换机上

在交换机的上联端口添加ARP信任命令，因为交换机的上连端口都是和其他合法的设备相连，设备与设备之间相连的端口必定是合法的。

但目前的ARP病毒层出不穷，已经不能单纯的依靠传统的方法去防范，比如简单的绑定本机ARP表，我们还需要更深入的了解ARP攻击原理，才能够通过症状分析并解决ARP欺骗的问题。

## （二）DHCP攻击应对措施

防DHCP攻击最常用的措施就DHCP SNOOPING。

DHCP Snooping技术是DHCP安全特性，通过建立和维护DHCP Snooping绑定表过滤不可信任的DHCP信息，这些信息是指来自不信任区域的DHCP信息。DHCP Snooping绑定表包含不信任区域的用户MAC地址、IP地址、租用期、VLAN-ID 接口等信息，如下表所示：

CORE4507#sh ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

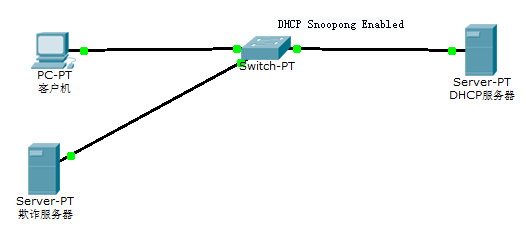
00:0D:60:2D:45:0D 10.149.3.13 600735 dhcp-snooping 100

GigabitEthernet1/0/7

这张表不仅解决了 DHCP用户的IP和端口跟踪定位问题，为用户管理提供方便，而且还供给动态ARP检测DA）和IP Source Guard使用。

关于DHCP SNOOPING，我们以学校CISCO-4507设备来演示：

首先定义交换机上的信任端口和不信任端口，对于不信任端口的 DHCP 报文进行截获和嗅探， DROP 掉来自这些端口的非正常 DHCP 报文，如下图所示：



基本配置示例如下表：

IOS 全局命令：

ip dhcp snooping vlan 10 针对10网段用户来开启DHCP SNOOPING

ip dhcp snooping 开启DHCP SNOOPING

接口命令

ip dhcp snooping trust 上连端口为合法接口

ip dhcp snooping limit rate 10

针对有些交换机没有DHCP SNOOPING功能，我们可以使用端口隔离技术，使交换机只能通过上连接口传输数据，本交换机端口之间不传输任何数据，这样也可以避免同一网段的用户获取到不合法的DHCP地址。

## （三）广播风暴应对措施

总的来看，要解决广播风暴的问题，可以从以下几个方面入手：

（1）在局域网中安装WSUS补丁服务器，保证局域网所有计算机都能及时打上最新的补丁。

（2）最好在局域网内安装网络版的防毒服务器，如无条件这，起码也得保证单机版的防毒软件的病毒库是经常更新的。

（3）检查每一台计算机的网卡、网线和交换机的每一个端口，检查是否有故障。

（4）当广播风暴发生时，观察交换机的指示灯不啻为很好的方法，可直接观察网络连通性及网络流量。

要避免广播风暴，可以采用恰当划分VLAN、缩小广播域、隔离广播风暴，还可在千兆以太网口上启用广播风暴控制，最大限度地避免网络再次陷入瘫痪。当端口接受到大量的广播、单播或组播的包时，就会发生广播风暴。转发这些包会导致网络速度变慢或超时，在交换机上借助对端口的广播风暴控制可以有效避免硬件损坏或链路故障导致的广播风暴的网络瘫痪。

以CISCO-2960设备为例，可在端口处添加

storm-control broadcast level 60.00 30.00

storm-control action shutdown

（当广播流量高于带宽的60%就自动关闭端口，当广播流量回落到30%以下就自动开启端口）

从实验结果来看，90%以上的网络广播风暴是病毒所致，因此，在局域网中配备防病毒系统，购置IDS入侵检测系统、网络流量检测工具等，以加强网络病毒的防治，加强对网络线路运行状态的监控，及时发现和处理网络上的异常流量和病毒攻击等问题，并制定计算机安全管理制度，确保网络线路的的正常运行。

# 五、结语

通过以上的措施，我们发现只要对网络进行合理的规划，适当的缩小虚拟网段，减小广播域，在底层交换机上的上连接口启用DHCP SNOOPING，或者是对底层交换机使用端口隔离技术，然后在对每个端口启用广播风暴控制，可有效的减少网络被攻击后造成的影响。

互联网络的飞速发展，对校园网络中师生的生活和学习已经产生了深远的影响，网络在我们的生活中无处不在。但是在享受高科技带来的便捷的同时，我们必须清醒的认识到，日益突出的网络安全问题也越来越成为网络应用的巨大阻碍，校园网络安全已经到了必须统一管理和彻底解决的地步，只有彻底解决网络安全问题，校园网的应用才能健康、高速发展。华中师大一附中校园网应该加强安全管理，增大安全管理的投入，共同做好校园网的安全管理工作，建设一个安全、可信的教育网络环境。