现代计算机技术与应用
2020 年 5 月第 2 卷第 2 期

# On the principle of ARP attack in campus network and Its Countermeasures

Wu Nanan

Fujian Normal University, Fuzhou

**Abstract:** Campus network plays a very important role in the school. However, ARP virus frequently occurs in campus network, which causes a lot of inconvenience for school staff to access the Internet. This paper introduces the principle and process of several common ARP deception and attack methods, and puts forward corresponding security precautions.

**Key words:** Campus network; address resolution protocol; ARP spoofing attack; network security

Received: 2020-03-18; Accepted: 2020-04-02; Published: 2020-04-04

文章引用：吴楠安. 浅议校园网 ARP 攻击的原理和防范对策 [J]. 现代计算机技术与应用，2020，2（2）：41–46.
https://doi.org/10.35534/mcta.0202007

# 浅议校园网 ARP 攻击的原理和防范对策

吴楠安

福建师范大学，福州

邮箱：naw2019@163.com

**摘　要：**校园网在学校中的作用非常重要，然而校园网中 ARP 病毒频繁发作，给学校工作人员上网造成诸多不便，本文介绍几种常见的 ARP 欺骗和攻击方式的原理及过程，并提出了相应的安全防范方法。

**关键词：**校园网；地址解析协议；ARP 欺骗攻击；网络安全

收稿日期：2020–03–18；录用日期：2020–04–02；发表日期：2020–04–04



ARP 欺骗攻击，是针对以太网地址解析协议的一种攻击技术。此种攻击可让攻击者取得局域网上的数据封包甚至可篡改封包，且可让网络上特定计算机或所有计算机无法正常连接。导致校园网的瞬间掉线或大面积的断网的情况多

数是由于 ARP 欺骗导致。比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。ARP 欺骗攻击只需成功感染一台计算机，就可能导致整个局域网无法上网，甚至可能使整个网络瘫痪。

# 1 ARP 欺骗分析

## 1.1 ARP 协议

ARP（Address Resolution Protocol）地址解析协议用于将计算机网络 IP 地址转化为物理 MAC 地址。ARP 协议的基本功能是根据计算机上的 IP 地址来查找本台机器的 MAC 地址。计算机上如果安装有 TCP/IP 协议，就会有一个用于存放 IP 地址与 MAC 地址对应关系的 ARP 缓存表，系统如果中 ARP 病毒，缓存表被修改，不断向路由器发送错误的 IP 或直接伪造一个虚假网关，那么整个网络就会出现频繁掉线现象。

## 1.2 ARP 协议的工作原理

局域网中同一网段甲乙两台计算机通讯，一台乙要和另一台甲进行通讯，首先需要知道甲的 MAC 地址。

乙计算机为了和甲通信，先要查找缓存中的 ARP 表，这个表示不断刷新的。如果当前该 ARP 表中没有相应的信息，那么计算机乙就必须先发出一个请求报文，该信息是以广播形式传播的。目的是询问：甲计算机的 MAC 地址是什么？

在整个局域网中的计算机全能收到乙发出来的请求报文，并检查自己的 IP 是不是要找的对象，如果是就响应，发送 ARP 响应报文，响应报文中有计算机甲的 MAC 地址。

## 1.3 ARP 协议自身的缺陷

按照 RFC 的规定，计算机在向网络发送 ARP 响应时，并不一定需要先收到网络上的 ARP 请求报文，任何一台计算机只要在局域网中就能向网络中的其他计算机发出通告：自己就是要查找的 MAC 地址的计算机，这样攻击者就有了可


https://doi.org/10.35534/mcta.0202007

乘之机。ARP 协议的缺陷，使攻击者发送虚假 ARP 请求和响应报文变得很容易，虚假的请求报文和响应报文能扰乱网络中被攻击主机的 ARP 表，这样就使得局域网中的合法主机无法在网络上通信。

很多黑客利用 ARP 协议的缓存更新不需要验证的特点，冒用一个局域网中合法的 IP，对同网络的数据进行试探，这正是 ARP 欺骗病毒所采用的手段。ARP 欺骗干扰网络连接通畅的方式分为两种，一种是欺骗路由器 ARP 表；另一种是欺骗内网计算机的网关。前一种 ARP 欺骗的原理是截获网关数据，它通过向路由器发送大量错误的内网 MAC 地址，而且反复重复不断进行，而真实的 MAC 地址信息就没有办法通过更新在路由器中保存，结果路由器所发送数据的对象就全部错误了；第二种 ARP 欺骗是通过伪造网关来实现欺骗。它的原理是建立虚假网关，让局域网中的计算机以为这个网关是真实网关，这样被它欺骗的计算机就会向假网关发送数据，这样就造成局域网络中的计算机断网掉线。

这种有目的的发布错误 ARP 广播包的行为，被称为 ARP 欺骗。ARP 欺骗，最初为黑客所用。黑客通过发布错误的 ARP 广播包，阻断正常通信，并将自己所用的电脑伪装成别人电脑，这样原本发往其他电脑的数据，就发到了黑客的电脑上，达到窃取数据的目的。

中期：ARP 恶意攻击

后来，有人利用这一原理，制作了一些所谓的“管理软件”，例如网络剪刀手、执法官、终结者等，这样就导致了 ARP 恶意攻击的泛滥。

现在：综合的 ARP 攻击

最近这一波 ARP 攻击潮，其目的、方式多样化，冲击力度、影响力也比前两个阶段大很多。

## 2　对 ARP 攻击的防护

防止 ARP 攻击是比较困难的，修改协议也是不可能。但有些工作是可以提高本地网络的安全性。

首先，如果一个错误记录被插入 ARP 或者 IProute 表，可以用两种方式来删除。1）使用 arp－dhost_entry；2）自动过期，由系统删除这样，可以采用以下

的一些方法：

## 2.1 减少过期时间

#ndd - set/dev/arparp_cleanup_interval60000

#ndd– set/dev/ipip_ire_flush_interval60000

60000=60000 毫秒默认是 300000

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

## 2.2 建立静态 ARP 表

可以建立如下文件并使用 arp - ffilename 命令加载进去：test.nsfocus.com 08：00：20：ba：a1：f2 user.nsfocus.com 08：00：20：ee：de：1f

这样建立的 ARP 映射是不过期的，也不会被刷新，当然可以使用 arp–d 来删除。但是这样会出现这样的情况，如果合法用户计算机网卡信息有变动，也不能接入网络。这时只有将这个 ARP 文件进行手工刷新才能是该用户接入网络。

## 2.3 完全禁止 ARP

可以用 ipconfiginterface - arp 命令来禁止 ARP 协议，禁止后，计算机网卡就不再发送和接受 ARP 包了。但是使用前提是使用静态的 ARP 表，如果不在 ARP 表中的计算机，将不能通信。对小规模的网络来说，还是有效可行的。

# 3 结语

由于 ARP 协议自身存在缺陷，ARP 攻击利用它给我们的网络造成了隐患，但是我们可以根据 ARP 病毒欺骗的基本原理，从多方面下手，消除隐患。只单一用一种方式来预防 ARP 攻击，可能不能完全保证我们网络的安全，如果能从客户端、服务器等多方面同时建立多种有效的防御措施，就能保证我们的网络远离 ARP 攻击。


https://doi.org/10.35534/mcta.0202007

## 参考文献

[1] 邓婉婷. 校园网 ARP 攻击检测系统设计与开发 [D]. 电子科技大学, 2011.

[2] 赵梦娜. 基于校园网的 ARP 攻击系统的设计与实现 [D]. 华南理工大学, 2014.

[3] 王帆. 浅谈校园网 ARP 攻击原理与防范 [J]. 信息与电脑：理论版, 2013（6）：11-12.