第 5 章　地址解析协议 ARP

本章学习目标：

- 理解 ARP 的工作机制(请求/响应模式)及缓存表原理。
- 掌握 ARP 报文格式及各字段功能。
- 熟悉 ARP 欺骗攻击原理及防御措施。

讨论完 IP 编址后，本章将重点探讨 IP 地址与物理地址的转换机制——地址解析。虽然互联网在逻辑层面通过 IP 地址实现了主机间的虚拟互联，但实际数据传输必须依赖物理网络完成。由于物理网络仅能识别 MAC 地址，因此需要专门的地址转换技术作为桥梁。地址解析协议(Address Resolution Protocol，ARP)是实现 IP 地址到 MAC 地址动态映射的关键技术，它弥补了 IP 在物理层适配的不足，使抽象的网络层寻址能够真正落实到具体的物理网络传输中。可以说，地址解析技术是维持 TCP/IP 协议栈上下层协作的重要纽带，没有它的支撑，基于 IP 的统一网络架构将难以在实际通信中发挥作用。

5.1　引言

在局域网(LAN)中，设备间的通信依赖数据链路层的 MAC 地址，而网络层使用的是 IP 地址。ARP 的核心作用在于实现这两者之间的映射：给定一个目标 IP 地址，ARP 通过协议交互获取对应的 MAC 地址，从而为数据帧的封装和传输提供必要信息。这一过程是二层通信的基础，直接影响网络的连通性与效率。

ARP 仅适用于局域网内部(同一广播域)，无法跨网段工作。对于跨网段通信，路由器会接管数据转发，而 ARP 的作用仅限于每个网段内的地址解析。此外，ARP 的实现依赖广播机制，这使其在小型网络中很高效，但在大型网络中可能因广播流量而增加带宽负担。

ARP 的应用无处不在。例如，在企业网络中，客户端通过 ARP 解析网关的 MAC 地址，以访问外部网络；在数据中心，服务器依赖 ARP 与交换机建立连接；在家庭网络中，路由器通过 ARP 为设备分配通信路径。这些场景凸显了 ARP 在网络通信中的基础地位。

5.2　为什么需要 ARP?

ARP 在网络通信中起着非常重要的作用，主要用于将网络层的 IP 地址解析为物理层的 MAC 地址，以便在本地局域网上正确地发送数据包。ARP 不能跨局域网被使用，只在本地局域网上起作用。

ARP 的作用主要体现在以下几方面。

(1) IP 地址与 MAC 地址转换。

在 TCP/IP 网络中，每个网络接口都有唯一的 MAC 地址和 IP 地址。当主机需要发送数据包到特定的 IP 地址时，需要知道该 IP 地址对应的 MAC 地址。地址解析协议将 IP 地

址解析为对应的 MAC 地址，实现了 IP 地址与 MAC 地址之间的转换。

(2) 局域网内通信。

在局域网中，主机之间的通信通常通过 MAC 地址直接通信。地址解析协议允许主机在同一局域网上查找并解析其他主机的 MAC 地址，确保数据包能够正确地发送到目标主机。

(3) 动态的网络环境。

网络中的主机可能加入或离开局域网，或者更改其网络接口的 MAC 地址。地址解析协议通过在局域网上动态更新 IP 地址与 MAC 地址之间的映射表，使网络能够适应这种变化，并确保数据包发送到正确的目标主机。

(4) 缓存机制提高性能。

地址解析协议使用一个缓存表来存储 IP 地址与 MAC 地址之间的映射关系，避免每次发送数据包都进行地址解析。当主机发送数据包时，首先检查本地 ARP 缓存表，如果找到对应的映射关系，就直接使用该 MAC 地址发送数据包，提高了网络传输的效率。

因此，ARP 在计算机网络中是必不可少的，它实现了 IP 地址与 MAC 地址之间的转换，确保数据包能够正确地发送到目标主机，并适应动态的网络环境，提高了网络通信的效率和可靠性。


5.3

5.3　ARP 的技术架构

5.3.1　ARP 的基本交互过程

ARP 的工作基于请求—应答机制，通常分为两个阶段。

(1) ARP 请求(request)。

发送方需要解析目标 IP 地址时，将构造一个 ARP 请求报文，并通过广播发送至局域网内所有设备。报文中包含发送方的 IP 和 MAC 地址、目标 IP 地址，以及全 0 的目标 MAC 地址(表示未知)。

(2) ARP 应答(reply)。

目标设备收到请求后，若发现目标 IP 与自身匹配，则通过单播返回 ARP 应答报文。报文中包含目标设备的 IP 地址和 MAC 地址。

例如，主机 A(IP：192.168.5.12，MAC：00:11:22:33:44:55)的广播请求是："谁是 192.168.5.20？请告诉我你的 MAC 地址。"主机 B(IP：192.168.5.20，MAC：00:AA:BB:CC:DD:EE)的回复是："我是 192.168.5.20，我的 MAC 地址是 00:AA:BB:CC:DD:EE。"

5.3.2　ARP 的报文格式

ARP 的报文格式如图 5-1 所示。

ARP 报文封装在以太网帧中，结构如下。

① **硬件类型(2B)**：表示网络类型，如以太网为 1。

② **协议类型(2B)**：表示上层协议，如 IP 为 0x0800。

③ **硬件地址长度(1B)**：通常为 6(以太网 MAC 地址)。

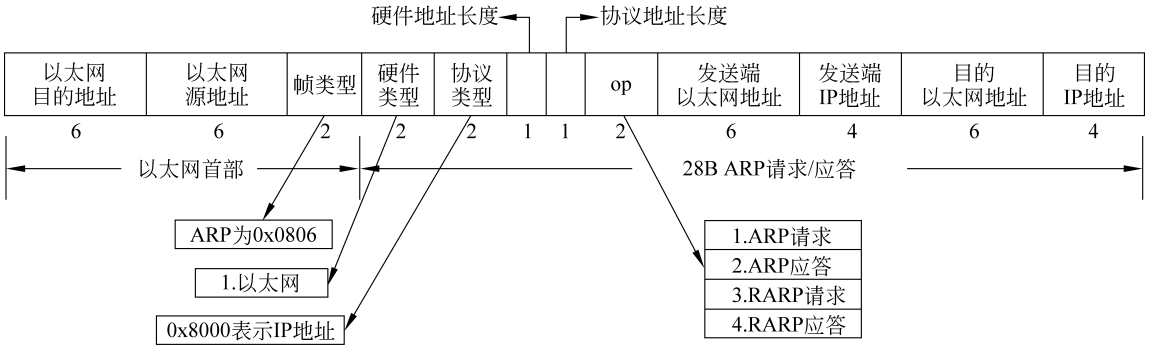

图 5-1　ARP 的报文格式

④ **协议地址长度(1B)**：通常为 4(IPv4 地址)。

⑤ **操作码(2B)**：1 表示请求，2 表示应答。

⑥ **发送方硬件地址/协议地址**：发送方的 MAC 地址和 IP 地址。

⑦ **目标硬件地址/协议地址**：目标主机的 MAC 地址和 IP 地址(请求时 MAC 地址为全 0)。

ARP 请求和响应报文的对比如表 5-1 所示。

表 5-1　ARP 请求和响应报文的对比

类型	目标 MAC 字段	传输方式	报文触发机制
ARP 请求	全 0 或全 F 广播地址	广播	本地缓存无对应表项时触发
ARP 响应	实际单播 MAC 地址	单播	收到与自身 IP 匹配的请求时响应

【例 5-1】 ARP 请求报文(操作码＝1)。

- 目标 MAC：FF:FF:FF:FF:FF:FF。
- 源 MAC：00:1A:2B:3C:4D:5E。
- 硬件类型：0x0001。
- 协议类型：0x0800。
- 操作码：0x0001。
- 发送方 MAC：00:1A:2B:3C:4D:5E。
- 发送方 IP：192.168.1.10。
- 目标 MAC：00:00:00:00:00:00。
- 目标 IP：192.168.1.20。

响应报文将替换目标 MAC 为实际地址，并设置操作码＝2。

5.3.3　ARP 的工作机制

IP 地址将物理地址对上层隐藏起来，使互联网表现出统一的地址格式，但是在实际网络通信时，IP 地址不能被物理网络所识别，物理网络依然使用物理地址，需要实现 IP 地址对物理地址的映射。对于以太网而言，当 IP 数据包通过以太网发送时，以太网链路并不识别 32 位 IP 地址，而是以 48 位 MAC 地址表示该以太网结点。因此，需要在 IP 地址与

MAC 地址之间建立映射关系(MAP),而建立这种映射的过程被称为地址解析(resoloution)。

如图 5-2 所示,假设 HostA 和 HostC 在同一个网段,HostA 要向 HostC 发送 IP 包,其地址解析过程如下。

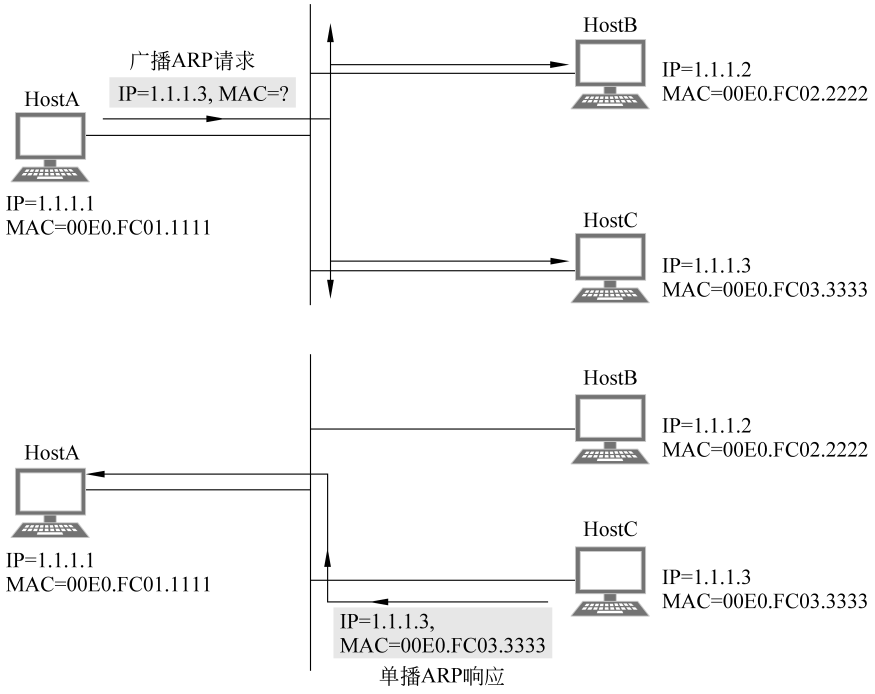

图 5-2　ARP 的工作机制

(1) HostA 首先查看自己的 ARP 表项,确定其中是否包含 HostC 的 IP 地址对应 ARP 表项。如果找到了对应的表项,则 HostA 直接利用 ARP 表项中的 MAC 地址将 IP 数据包封装成帧,并将帧发送给 HostC。

(2) 如果 HostA 在 ARP 表中找不到对应的表项,则暂时缓存该数据包,然后以广播方式发送一个 ARP 请求。ARP 请求报文中的发送端 IP 地址和发送端 MAC 地址为 HostA 的 IP 地址和 MAC 地址,目标 IP 地址为 HostC 的 IP 地址,目标 MAC 地址为全 0 的 MAC 地址。

(3) 由于 ARP 请求报文以广播方式发送,该网段上的所有主机都可以接收到该请求。HostC 比较自己的 IP 地址和 ARP 请求报文中的目标 IP 地址,由于两者相同,HostC 将 ARP 请求报文中的发送端(HostA)IP 地址和 MAC 地址存入自己的 ARP 表中,并以单播方式 HostA 发送 ARP 响应,其中包含了自己的 MAC 地址。其他主机发送请求的 IP 地址并非自己的,于是都不作应答。

(4) HostA 收到 ARP 响应报文后,将 HostC 的 MAC 地址加入自己的 ARP 表中,同时将 IP 数据包用此 MAC 地址为目的地址封装成帧,并发送给 HostC。

对于不同的链路,需要使用代理 ARP。通常 ARP 会被路由器隔离,但是采用代理 ARP(ARP Proxy)的路由器可以将 ARP 请求转发给临近的网段,使多个网段中的结点像是在同一网段内通信。

5.3.4 ARP 高速缓存

现在知道了发送一次 IP 分组前通过发送一次 ARP 请求就能够确定 MAC 地址。那么是不是每发送一次都得经过广播→封装 ARP 响应→返回给主机这一系列流程呢？想想看，浏览器是如何做的呢？

答案是浏览器内置了缓存，它能够缓存最近经常使用的地址，ARP 也是一样。ARP 高效运行的关键就是维护每个主机和路由器上的 ARP 高速缓存(或表)。这个缓存维护着每个 IP 地址到 MAC 地址的映射关系，通过把第一次 ARP 获取到的 MAC 地址作为 IP 对 MAC 的映射关系到一个 ARP 缓存表中，下一次再向这个地址发送数据报时就不再需要重新发送 ARP 请求了，而是直接使用这个缓存表中的 MAC 地址进行数据报的发送。每发送一次 ARP 请求，缓存表中对应的映射关系都会被清除。通过 ARP 高速缓存降低了网络流量的使用，在一定程度上防止了 ARP 的大量广播。

一般来说，发送过一次 ARP 请求后，再次发送相同请求的概率比较大，因此使用 ARP 缓存能够减少 ARP 包的发送。除此之外，不仅 ARP 请求的发送方能够缓存 ARP 接收方的 MAC 地址，接收方也能够缓存 ARP 请求方的 IP 和 MAC 地址，如图 5-3 所示。

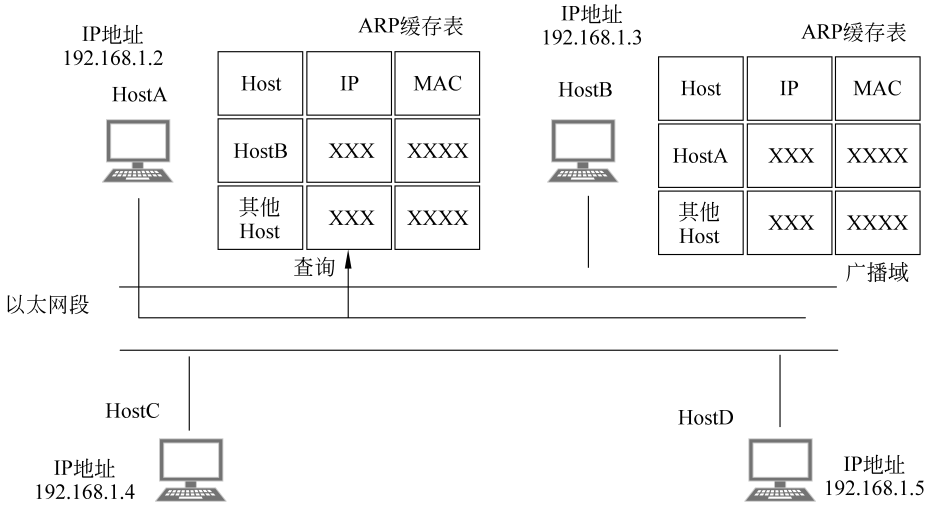

图 5-3 ARP 缓存机制

不过，MAC 地址的缓存有一定期限，超过这个期限后，缓存的内容会被清除。

在 Linux 或者 Windows 中可以使用 arp 命令查看 ARP 缓存。在 Windows 中的 DOS 命令提示符下，ARP 命令的形式如下：

```
C:\Documents and Settings\Administrator>arp - *
```

其中“*”表示参数。ARP 命令参数及相应的功能如表 5-2 所示。选项-a 用于显示系统缓存中所有的缓存项。需要说明的是，ARP 命令仅对 ARP 缓存操作，不会发送 ARP 请求。

表 5-2　ARP 命令

参　　数	含　　义
-a	列出 ARP 缓存中的所有条目
-a lnet_addr	列出与 lnet_addr 对应的条目
-d lnet_addr	删除与 lnet_addr 对应的条目
-s lnet_addr eth_addr	在 ARP 缓存中添加一个条目

【例 5-2】 在 Linux 中使用 arp 查询缓存如图 5-4 所示。

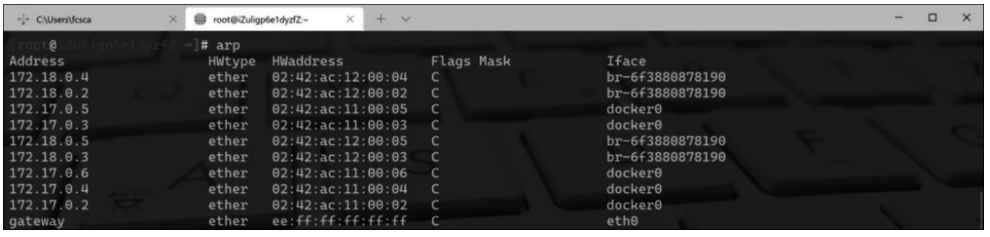

图 5-4　Linux 中使用 arp 查询缓存

主要包含以下 5 项。

- 主机名：对应一个 IP 地址。
- 硬件地址类型。
- 硬件地址。
- 标志。
- 本地网络接口。

标志主要分为 3 类：C、M 或 P，C 表示的是由 ARP 动态学习。M 类可以通过 arp-s 增加一条。P 类表示的是发布，对于任何 P 类项目，主机对输入的 ARP 请求都返回一个 ARP 响应。这个选项用于配置代理 ARP。

在 Windows 中进行 ARP 缓存查询如图 5-5 所示。

图 5-5　Windows 中使用 ARP 查询缓存

Windows 中的 ARP 程序显示了 IPv4 的地址，它的接口是十六进制数，Windows 版本还指出地址是手动输入还是 ARP 动态学习的。在上面的例子中，既有静态的也有动态的，

48 位的 MAC 地址被显示为 6 个十六进制数,在 Linux 中使用“:”,在 Windows 中使用“-”进行分隔。

5.3.5 用 ARP 实现地址冲突检测

某些读者可能会有这样的经历:当你手工为某个主机配置一个 IP 地址,而这个 IP 地址又正在被其他主机使用时,两台主机的操作系统会同时提示 IP 地址冲突。IP 地址冲突是非法的,使用 ARP 则可以对可能发生的冲突进行检测。

(1) 基本的地址冲突检测方法。

在 RFC2131 中,DHCP 标准初步给出了使用 ARP 检测冲突的方法:当 DHCP 服务器给某个主机分配 IP 地址后,这台主机广播 ARP 报文,将其中的“发送方物理地址”和“发送方 IP 地址”分别设置为自己的物理地址和全 0;“目的 IP 地址”字段则设置为分配给自己的 IP 地址。如果主机收到回应,说明此 IP 地址已经被占用,则向 DHCP 服务器发送 DHCPDECLINE 消息,以通告 IP 地址冲突。RFC2131 给出的这种方案存在两个问题:一是其适用于使用 DHCP 动态分配 IP 地址的场合;二是它只给出了这个思想,而未给出应答超时如何设置、发现 IP 地址冲突后应如何处理等诸多问题的细节。正是由于这些问题,2008 年 7 月,一个专门描述 IP 地址冲突的 RFC 问世,即 RFC5227——IPv4 地址冲突检测(Address Conflict Detection, ACD)。

(2) ACD。

ACD 定义了 ARP 探测报文和通告报文,这二者都是 ARP 请求报文,但内容设置和功能不同。前者用于检测 IP 地址冲突,其内容设置和使用方法与前述 DHCP 报文给出的方案相同。需要说明的是,将“发送方 IP 地址”设置为全 0 是为了防止对其他主机的 ARP 缓存造成“污染”,因为如果当前 IP 地址已经被其他主机使用,这个 IP 地址与 MAC 的映射关系就是非法的。通告报文则用于通告子网内其他主机自己的新 IP 地址即将使用,其“发送方 IP 地址”和“目的 IP 地址”字段都设置为主机自己的 IP 地址。

ACD 的流程如下。

① 当主机的一个 IP 地址被激活时(当系统启动、IP 地址重新配置或连接建立时),主机会发送一个 ARP 探测报文。

② 如果收到了 ARP 应答,说明该 IP 地址已经被占用;如果收到了一个“目的 IP 地址”字段也是该 IP 地址的探测报文,说明另外一台主机也想使用这个地址。无论收到何种报文,两台主机都会提醒用户出现地址冲突。此时主机有 3 种选择:一是放弃使用该 IP 地址;二是发送一个通告报文对该地址进行“守卫”,如果仍然冲突,则放弃这个 IP 地址;三是无视冲突,继续使用。

③ 如果未收到上述两种报文,说明 IP 地址可用。主机会发送 ARP 通告,用以通告自己的 IP 和 MAC 地址的映射关系。

④ 在系统运行期间,ACD 一直在运行,以进行地址冲突检测。

除上述基本流程外,RFC5227 还定义了若干所需的时钟以及最大冲突数限制等。比如,PROBE_MIN 为 1s,给出了探测报文等待回应的最小时间间隔;PROBE_MAX 为 2s,是最大时间间隔。

(3) Gratuitous ARP。

Gratuitous ARP 在中文文献中通常被翻译为“免费 ARP”或“无故 ARP”，笔者认为这种翻译过于拗口，所以仍以英文词描述。Gratuitous ARP 是一种通告机制，用以通知其他主机更新 ARP 缓存，以存放 Gratuitous ARP 报文发送端的最新地址映射关系。这个通告报文既可以是 ARP 请求报文，也可以是应答报文，具体可由实际的应用场景指定，但通常都是请求报文。很多文献将 Gratuitous ARP 也作为一种 IP 地址冲突检测机制，但是笔者认为 Gratuitous ARP 只是一个框架，ACD 的探测和通告报文都可以看作 Gratuitous ARP。

有关使用 ARP 实现 IP 地址冲突检测的内容就讨论至此。在这里，我们留一个问题：如果两台主机的物理地址不同，但设置了同样的 IP 地址，这样系统必然会提示 IP 地址冲突。但是，如果想办法让两台主机的 IP 地址和物理地址都相同，会出现什么情况呢？请读者自行试验并给出答案。

5.4　ARP 的安全性分析


5.4

ARP 缓存的设置有效提高了通信效率，但它也为使用 ARP 的网络带来了安全风险。ARP 欺骗是目前常见的攻击手段，它是在交换式网络环境下实施嗅探及会话劫持的基础。

5.4.1　嗅探器的原理

在众多的网络攻击方法中，嗅探是一种常见而隐蔽的手段。攻击者可以利用这种技术获取网络中的通信数据。回忆以太网的工作机制，在共享式环境下(比如用集线器连接所有设备)，所有数据都以广播方式发送，所有主机共享同一信道。这里的广播指硬件广播，是物理介质传递数据信号的方式，而不是指把物理帧的“目的物理地址”字段设置为物理广播地址。在一般工作模式下，网卡会把物理帧的“目的物理地址”字段与自己的地址相比较。一致时会接收帧，否则忽略之。当网卡工作于混杂(promiscuous)模式时，不进行这种检查，它会接收网络中的所有数据。因此，在共享网络环境下，通过设置网卡的工作模式即可嗅探网段内所有的通信数据。而使这种攻击成为可能的本质原因就是硬件广播投递方式。

防范这种攻击的有效途径之一就是采用交换式网络架构，因为交换机具有记忆功能。它把每个端口与该端口所连设备的物理地址进行绑定，并依据帧首部的目的物理地址把数据直接发送到相应端口，抛弃了共享环境下的广播方式。从防范嗅探的角度看，交换式网络环境似乎优于共享环境，但 ARP 给它带来了另一种风险。

5.4.2　基于 ARP 欺骗的嗅探器及会话劫持

ARP 欺骗是攻击者在交换式网络环境下实施嗅探的基础，下面通过一个示例来说明其原理。假设网络中有一台主机 H，它要嗅探 A 和 B 之间的通信数据。3 台主机的 IP 地址分别为 IPH、IPA 和 IPB，物理地址分别为 MACH、MACA 和 MACB。H 首先向 A 发送一个 ARP 应答报文，其中包含的映射关系为 IPB/MACH，A 收到这个应答后，更新自己的缓存，保存映射关系 IPB/MACH；随后，H 向 B 发送一个 ARP 应答报文，其中包含的映射关系为 IPA/MACH，B 收到这个应答后，更新自己的缓存，保存映射关系 IPA/MACH。当 A 向 B 发送数据时，物理帧的目的物理地址将被设置为 MACH，反之亦然。至此，A 和 B 之间的所

有通信数据都将发送给 H。

在截获了重要的通信数据后,H 可以把数据转发到正确的目的地,而 A 和 B 都无法察觉嗅探行为。鉴于 ARP 缓存会定期更新,H 只要以小于更新时间间隔的频率发送 ARP 欺骗报文,就可以持续嗅探 A 和 B 之间的数据。

除嗅探外,基于 ARP 还可实现会话劫持及恶意代码植入。事实上,攻击者利用 ARP 欺骗技术截获数据后,即可在转发数据前更改数据。如果在 Web 访问应答报文中插入恶意代码,就可以通过浏览器对这段代码的解释来达到木马植入的目的。

5.4.3 ARP 欺骗的防范

防范 ARP 欺骗的途径之一就是使用静态缓存。在 DOS 下设置静态 ARP 缓存表项的命令是“arp -s IP MAC”,在 Cisco 下的命令为“arp IP mac arpa intID”,即在 intID 接口上只能使用指定的 IP 和 MAC 地址。除手工配置外,互联网上也有很多免费工具提供 ARP 静态绑定功能。

除上述方式外,也可以使用 ARP 卫士等专门的 ARP 欺骗防范工具。ARP 卫士在系统底层安装了一个核心驱动,通过这个驱动过滤所有的 ARP 数据包。它会对每个 ARP 应答进行判断,只有符合规则的 ARP 报文才会被进一步处理。同时 ARP 卫士会对每个发送出去的 ARP 应答进行检测,只有符合规则的 ARP 数据包才会被发送出去,从而防止了发送攻击报文。互联网上有诸多免费的 ARP 防火墙工具,感兴趣的读者可进一步搜索使用。

从防范嗅探的角度看,可以对数据进行加密处理。这就确保了即便攻击者截获了数据,也无法查看和更改数据的内容。

5.5 典型攻防案例

5.5.1 ARP 静态绑定与双向断网攻击

1. 攻击过程

(1) 攻击者在 PC1 上使用网络监控软件向目标主机 PC2 发送伪造的 ARP 响应,将自身伪装成网关,导致 PC2 的 ARP 表被污染,进而无法访问互联网。

(2) 网络管理员发现异常后,在 PC2 上通过命令静态绑定网关的真实 IP-MAC 地址,暂时恢复网络通信。

(3) 攻击者更改监控软件的攻击模式为“双向断开”,同时篡改 PC2 的 ARP 缓存表和网关的 ARP 表,使得即使存在静态绑定,PC2 仍无法正常联网。

2. 防御措施

(1) 静态绑定+ARP 防火墙。

在主机上通过命令(如 arp -s)绑定网关的 IP-MAC 地址,并安装 ARP 防火墙实时监测异常 ARP 报文,拦截非法修改请求。

(2) 动态 ARP 检测(DAI)。

在交换机上启用 DAI 功能,通过验证 ARP 报文的合法性(如 IP-MAC 绑定关系)阻断伪造包传输。

5.5.2　中间人攻击与 DNS 劫持组合

1. 攻击过程

(1) 攻击者扫描企业内网,获取网关和员工主机的 IP-MAC 信息。

(2) 使用 Scapy 工具发送伪造的 ARP 响应,将网关 IP 映射到攻击者 MAC,实现流量劫持。

(3) 拦截员工主机的 DNS 请求,将特定域名解析结果篡改为攻击者控制的恶意服务器 IP,诱导用户访问钓鱼网站。

2. 防御措施

(1) 加密通信协议。

采用 HTTPS、DNSSEC 等加密协议,防止流量被篡改或监听。

(2) 网络分段与监控。

划分 VLAN 限制广播域,部署 IDS/IPS 检测异常 ARP 流量和 DNS 响应异常。

5.5.3　长角牛软件 ARP 欺骗

1. 攻击过程

(1) 攻击者配置虚拟机与真机在同一局域网(如 VMnet1),手动设置 IP 地址为 192.168.226.100 和 192.168.226.101。

(2) 在攻击机上运行长角牛软件,选择目标主机(如 192.168.226.101),设置“禁止用户”权限并勾选管理选项,阻断其与网关的通信。

(3) 目标主机尝试 ping 网关时,因 ARP 表被篡改而显示“请求超时”。

2. 防御措施

(1) 静态路由配置。

通过命令 netsh interface ipv4 add neighbors 绑定网关的 IP-MAC 地址,防止动态 ARP 表被覆盖。

(2) 物理隔离与权限控制。

对高危操作(如安装网络监控软件)限制管理员权限,并隔离实验环境与生产网络。

以上案例体现了 ARP 攻击的多样性和防御的层次性,需结合静态绑定、动态检测、加密协议等多维度策略应对。

5.6　本章小结

本章不仅深入讲解了 ARP 的工作原理、报文格式及其在网络通信中的重要作用,还讲解了 ARP 欺骗攻击及其防范措施。这些内容不仅丰富了我们的计算机网络知识,更蕴含了深刻的网络道德与安全意识。

① **网络道德**:ARP 作为局域网通信的基础,其正常运作依赖网络中各主机的诚信与合作,任何一台主机故意发送伪造的 ARP 报文,都会破坏整个网络的通信秩序,影响其他主机的正常使用,这要求我们在网络空间中也要遵循基本的道德规范,诚实守信,不损害他人利益。