ARP 欺骗攻击的几种常见类型及防御

ARP 定义

ARP（Address Resolution Protocol）是地址解析协议，是一种将 IP 地址转化成物理地址的协议。

ARP 原理

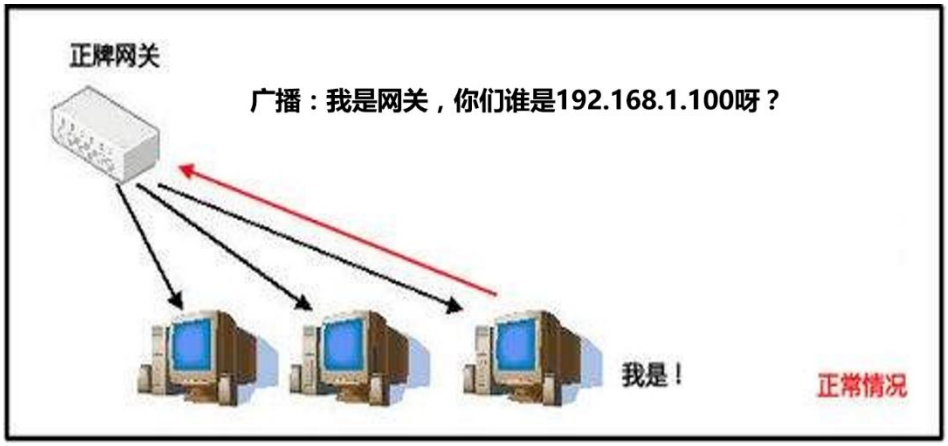


图 1 正常 ARP 情况

某机器 A 要向主机 B 发送报文，会查询本地的 ARP 缓存表，找到 B 的 IP 地址对应的 MAC 地址后，就会进行数据传输。如果未找到，则 A 广播一个 ARP 请求报文，所有主机都收到 ARP 请求，主机 B 识别自己的 IP（192.168.1.100）地址，向 A 主机发回一个 ARP 响应报文。其中就包含有 B 的 MAC 地址，A 接收到 B 的应答后，就会更新本地的 ARP 缓存，接着使用这个 MAC 地址发送数据。

ARP 欺骗和攻击的类型

1、冒充网关

ARP病毒通过发送错误的网关MAC对应关系给其他受害者，导致其他终端用户不能正常访问网关,见图 2 ：

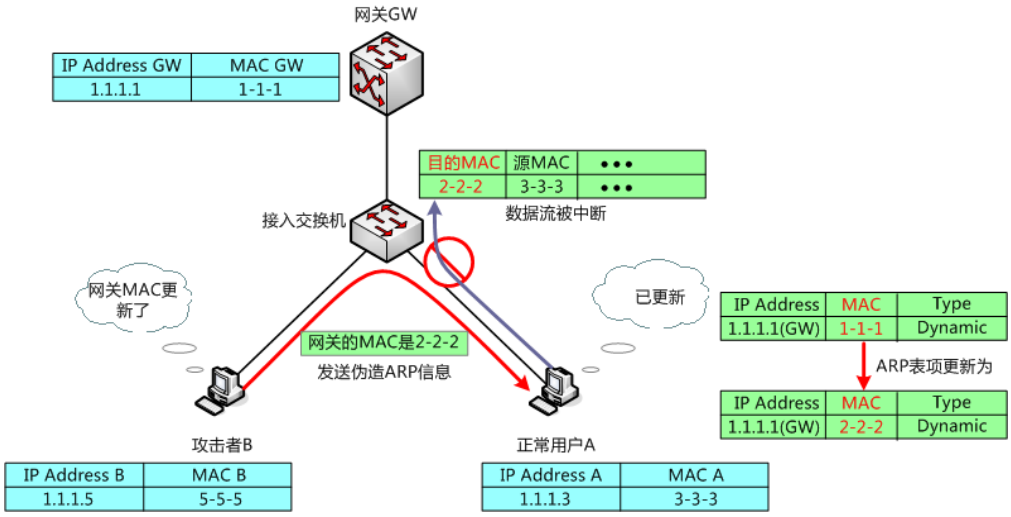
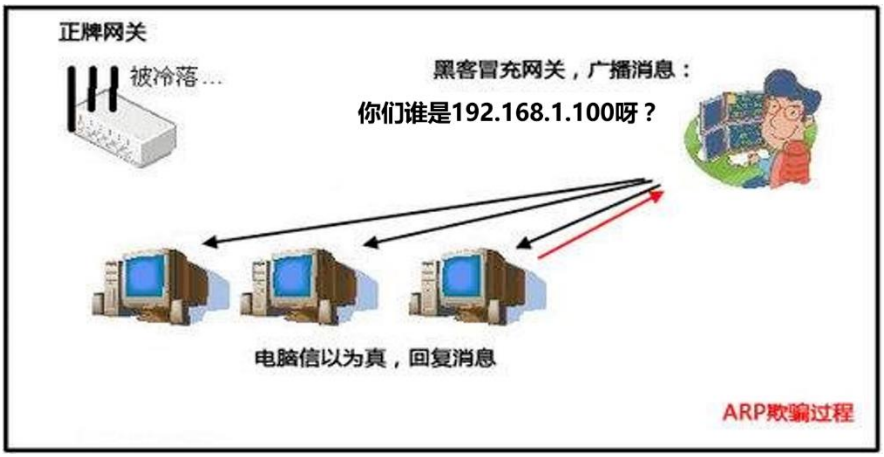


图 2 网关冒充攻击示意图

如上图所示，攻击者发送伪造的网关ARP报文，欺骗同网段内的其它主机。从而网络中主机访问网关的流量，被重定向到一个错误的MAC地址(这个错误的MAC地址可以是攻击者自身的MAC地址，也可以构造一个网络中其他主机或是一个不存在的MAC地址，主要还是看攻击者的最终目的是什么)，导致该用户无法正常访问外网。



2、欺骗网关

攻击者发送错误的终端用户的IP＋MAC的对应关系给网关，导致网关无法和合法终端用户正常通信。见图3：

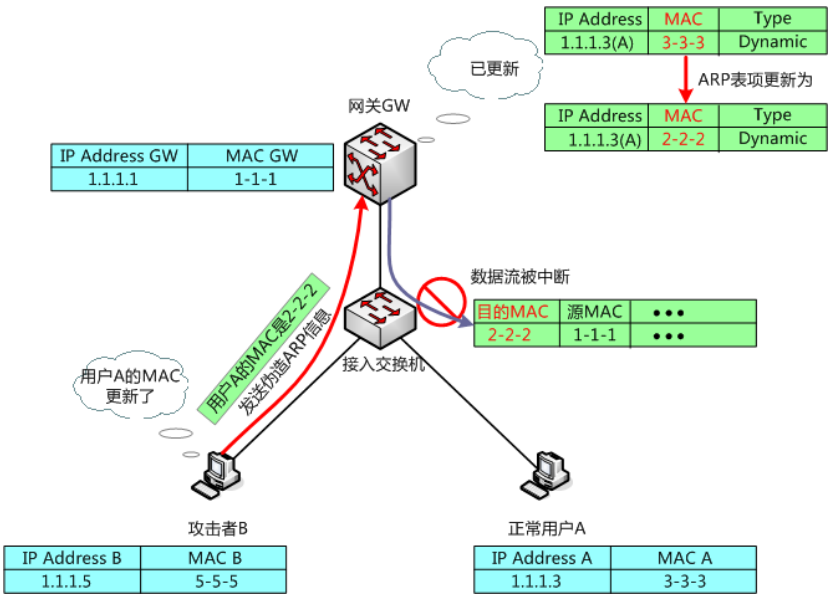


图 3 欺骗网关攻击示意图

如上图，攻击者伪造虚假的ARP报文，欺骗网关相同网段内的某一合法用户的MAC地址已经更新。网关发给该用户的所有数据全部重定向到一个错误的MAC地址，导致该用户无法正常访问外网。

3、欺骗终端用户

这种攻击类型，攻击者发送错误的终端用户/服务器的IP＋MAC的对应关系给受害的终端用户，导致同网段内两个终端用户之间无法正常通信，见图4：

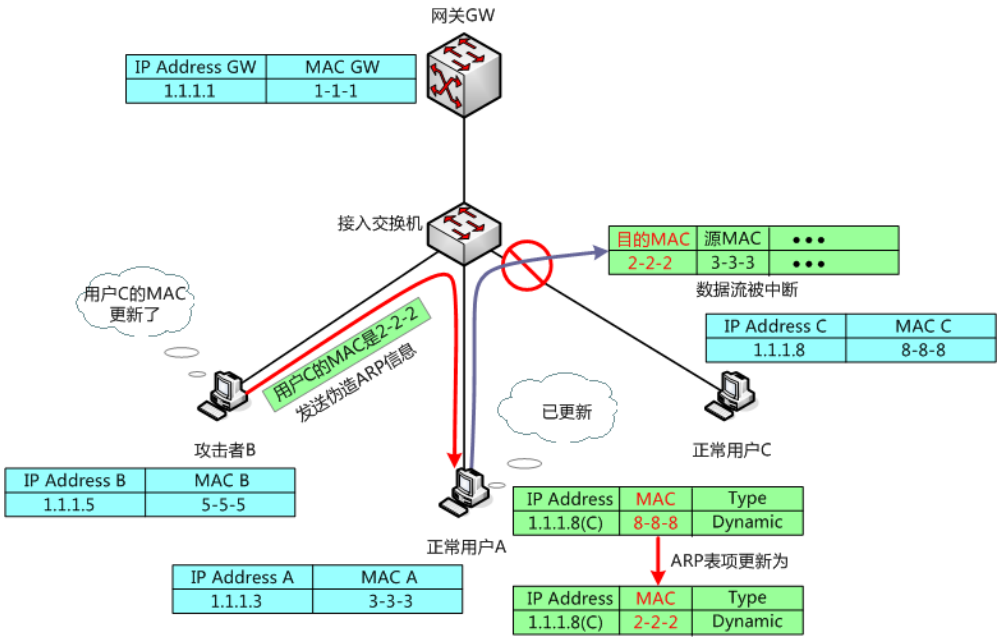


图4 欺骗终端攻击示意图

如上图，攻击者伪造虚假的ARP报文，欺骗相同网段内的其他主机该网段内某一合法用户的MAC地址已经更新。导致该网段内其他主机发给该用户的所有数据全部重定向到一个错误的MAC地址，导致同网段内的两台主机无法正常通信。

4、ARP 泛洪攻击

这种攻击类型，攻击者伪造大量不同ARP报文在同网段内进行广播，导致网关ARP表项被占满，合法用户的ARP表项无法正常学习，导致合法用户无法正常访问外网。主要是一种对局域网资源消耗的攻击手段。如下图：

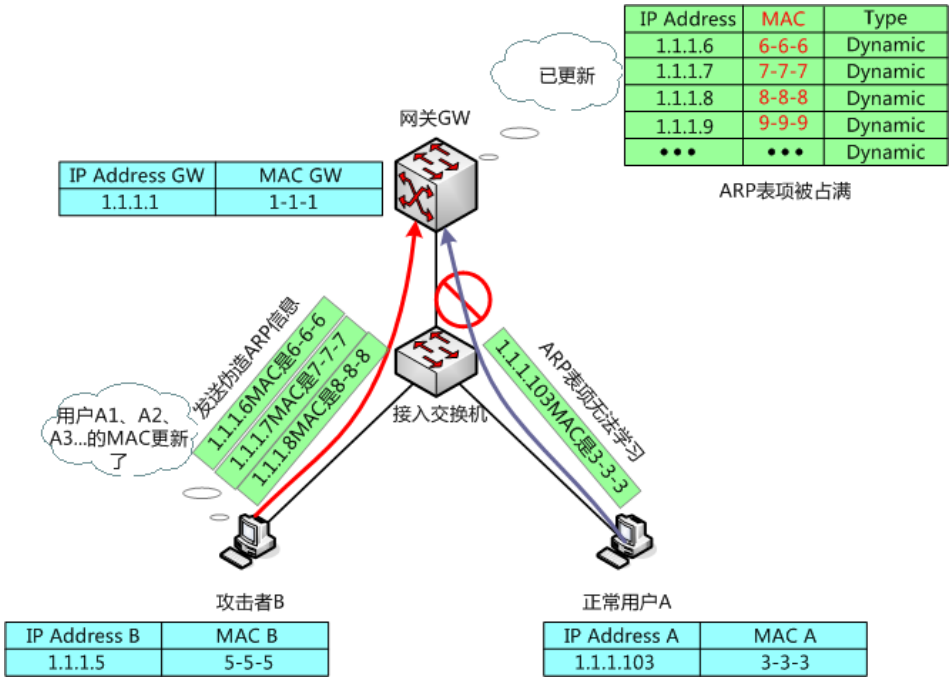


图 5 ARP泛洪攻击示意图

典型应用

通过对上述的 ARP 欺骗和攻击类型的介绍。我们可以很容易发现当前 ARP 欺骗和攻击防御的关键所在：如何获取到合法用户和网关的 IP+MAC 对应关系，并如何利用该对应关系对 ARP 报文进行检查，过滤掉非法 ARP 报文，解决客户网络受到 ARP 攻击的问题。

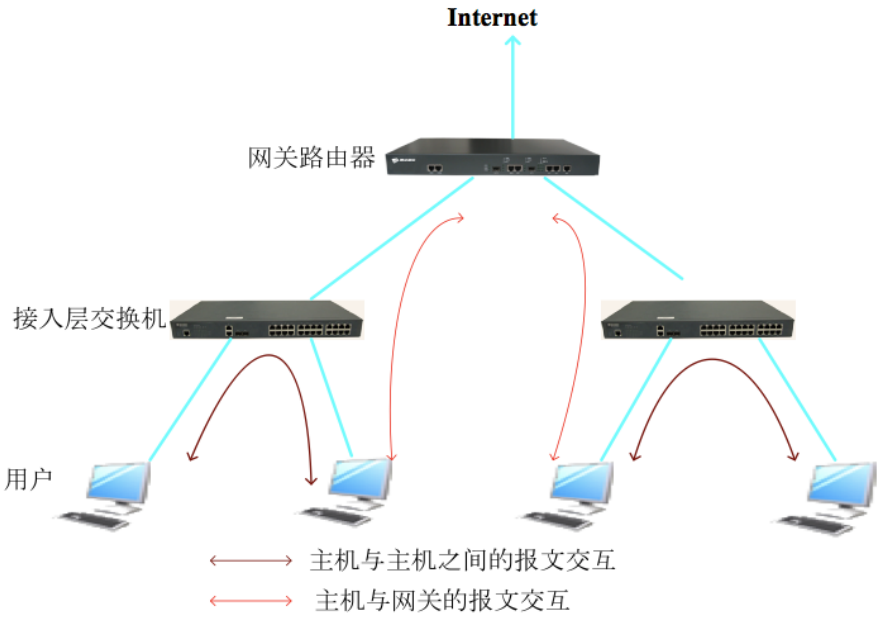


图 6 ARP 报文交互示意图

如图 6 所示，ARP 攻击防范技术的思路是以设备角色为线索，通过分析二三层网络设备可能会面对哪些类型的攻击，从而提供有效的防范措施。

攻击源一般来自于主机侧，因此无线接入点或者接入交换机在 ARP 攻击防范中是一个关键的控制点。针对攻击的特点，主要从两个方面考虑：

1. 建立正确的 ARP 映射关系、检测并过滤伪造的 ARP 报文，保证经过其转发的 ARP 报文正确合法。

2. 抑制短时间内大量 ARP 报文的冲击。

由于防范措施部署在接入侧，因此无需在网关上部署，可以减轻网关负担。