# 计网实验报告1

## 实验1：交换机的基础配置

### 一、实验目的

交换机的基础配置

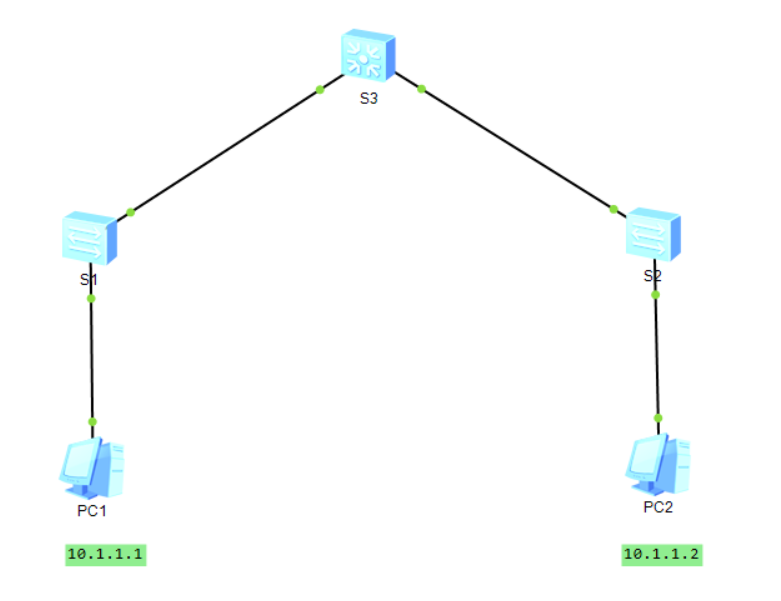
* 理解双工模式和接口速率

* 掌握更改双工模式的配置

* 掌握更改接口速率的配置

### 二、实验环境

**基础配置拓扑：**



**实验编址：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 子网掩码 | 默认网关 |
| PC-1 | Ethernet 0/0/1 | 10.1.1.1 | 255.255.255.0 | N/A |
| PC-2 | Ethernet 0/0/1 | 10.1.1.2 | 255.255.255.0 | N/A |

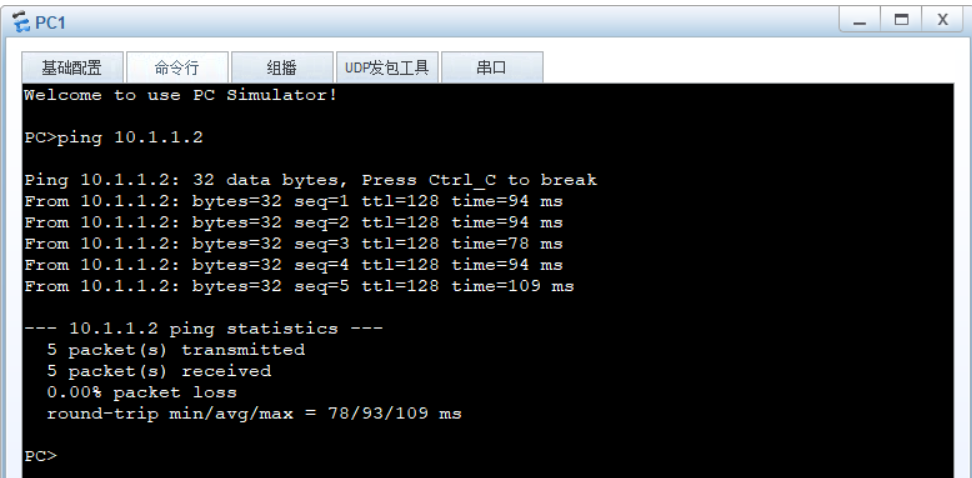
### 三、实验内容

某公司刚成立，新组建网络，购置3台交换机，其中S1和S2为接入层交换机，S3为汇聚层交换机。现在网络管理员需要对3台新交换机进行基本配置，保证交换机间的接口使用全双工模式，并根据需要配置接口速率。

### 四、实验结果

1. 基本配置

根据实验编址表进行相应的基本 IP 配置，并使用 ping 命令检测各直连链路的连通性



发现 PC-1 与 PC-2 之间能 ping 通，说明能正常通信

1. 配置交换机双工模式

配置接口的双工模式可在**自协商**或者**非自协商**模式下进行。

在自协商模式下，接口的双工模式是和对端接口协商得到的，但协商得到的双工模式可能与实际要求不符。可通过配置双工模式的取值范围来控制协商的结果。例如，互连的两个设备对应的接口都支持全/半双工，经自协商后工作在半双工模式，与实际要求的全双工模式不符，这时就可以执行 **auto duplex full** 命令使接口的可协商双工模式变为全双工模式·默认情况下，以太网接口自协商双工模式范围为接口所支持的双工模式。

在非自协商模式下，可以根据实际需求手动配置接口的双工模式。在S1、S2、S3交换机接口下先通过 **undo negotiation auto** 命令关掉自协商功能，再手工指定双工模式为全双工。

**全双工模式配置：**

**undo info enable //信息不显示**

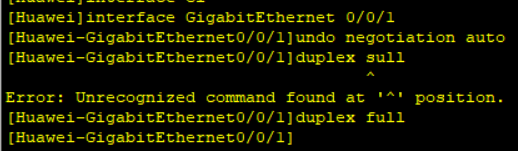
**sys //进入系统视图**

**interface GigabitEthnet 0/0/1 //进入接口**

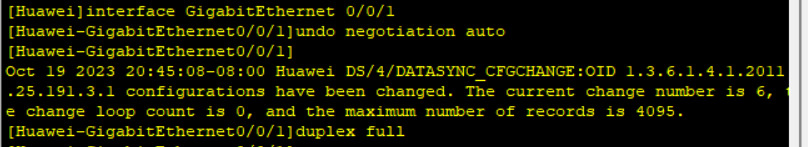
**undo negotiation auto //关掉自动协商功能**

**duplex full //全双工**

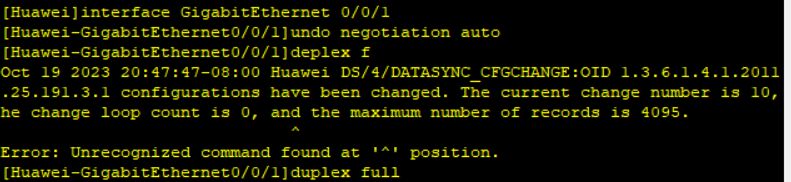
S1 配置

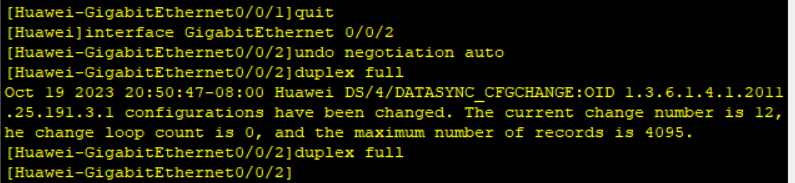


S2 配置



S3 配置





1. 配置接口速率

在自协商模式下，以太网接口的速率是和对端接口协商得到的。如果协商的速率与实际要求不符，可通过配置速率的取值范围来控制协商的结果。例如，互连的两个设备对应的接口经自协商后的速率为 **10Mbit/s**，与实际要求的 **100Mbit/s** 以不符，可通过执行**auto speed 100**命令配置使得接口可协商的速率为 **10Mbit/s** 。默认情况下，以太网接口自协商速率范围为接口支持的所有速率。

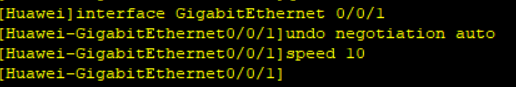
在非自协商模式下，需手动配置接口速率，避免发生无法正常通信的情况。

默认情况下，以太网接口的速率为接口支持的最大速率。

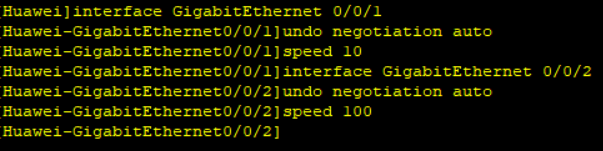
根据网络需要调整接口速率、由于网络用户较少，配置 GE 接口速率为 **100Mbit/s** ，配置 Ethernet 接口速率为 **10Mbit/s**。

在3台交换机接口下配置速率。首先关闭接口自协商模式，然后配置以太网接口的速率。

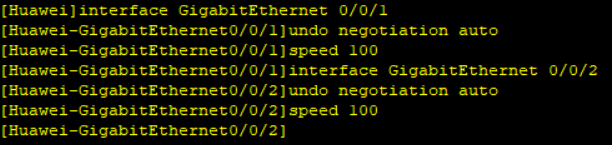
S1 配置



S2 配置



S3 配置



### 五、讨论与分析

**思考**

**在实际操作中，通常使用自动协商模式还是手动配置模式？为什么？**

在大多数普通网络中，自动协商模式通常更推荐，因为它提供了便捷性、灵活性，并且能够适应不同设备的连接。但在某些特殊需求或对网络稳定性要求极高的环境中，手动配置模式可能更合适。在实际操作中，选择哪种模式通常需要综合考虑网络的需求、设备的兼容性和稳定性。

**收获**

通过这次实验了解了如何配置交换机的全双工模式和接口速率，通过配置合适的双工模式和接口速率，可以最大限度地利用网络带宽，并确保数据在网络中的流动是高效和可靠的。

## 实验2：理解 ARP 及 Proxy ARP

### 一、实验目的

理解 ARP 及 Proxy ARP

* 理解 ARP 的工作原理

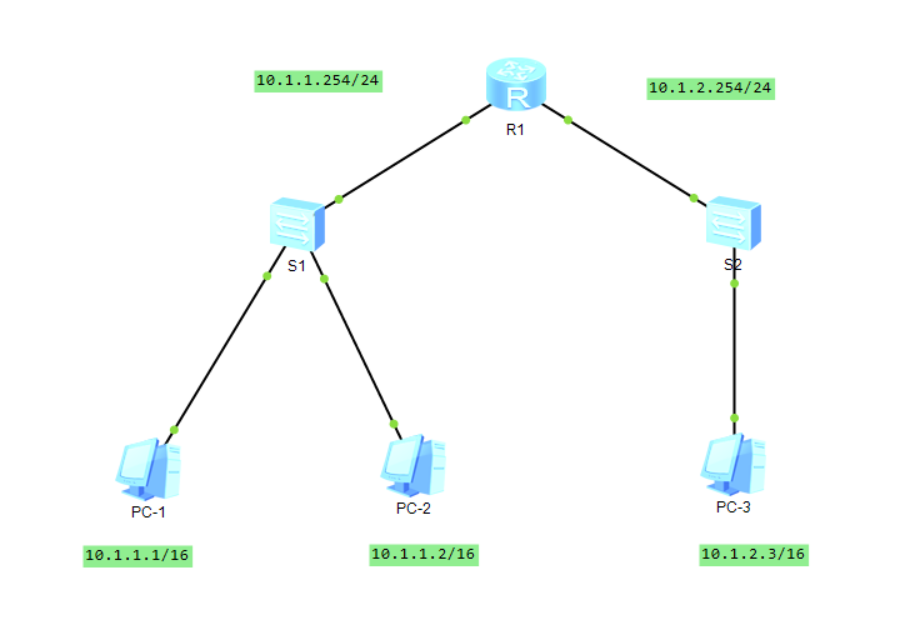
* 掌握配置静态 ARP 的方法

* 理解 Proxy ARP 的配置

* 理解主机之间的通信

### 二、实验环境

**实验拓扑：**



**实验编址：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 子网掩码 | 默认网关 |
| R1(AR220) | GE 0/0/1 | 10.1.1.254 | 255.255.255.0 | N/A |
| GE 0/0/2 | 10.1.2.254 | 255.255.255.0 | N/A |
| PC-1 | Ethernet 0/0/1 | 10.1.1.1 | 255.255.0.0 | N/A |
| PC-2 | Ethernet 0/0/1 | 10.1.1.2 | 255.255.0.0 | N/A |
| PC-3 | Ethernet 0/0/1 | 10.1.1.3 | 255.255.0.0 | N/A |

### 三、实验内容

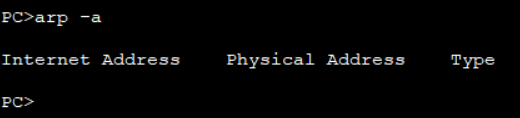
本实验模拟公司网络场景。路由器RI是公司的出口网关，连接到外网。公司内所有员工使用 10.1.0.0/16 网段，通过交换机连接到网关路由器上。网络管理员通过配置静态ARP防止ARP欺骗攻击，保证通信安全。又由于公司内所有主机都没有配置网关，且分属于不同广播域，造成无法正常通信，网络管理员需要通过在路山器上配置ARP代理功能，实现网络内所有主机的通信。

### 四、实验结果

1. 基本配置

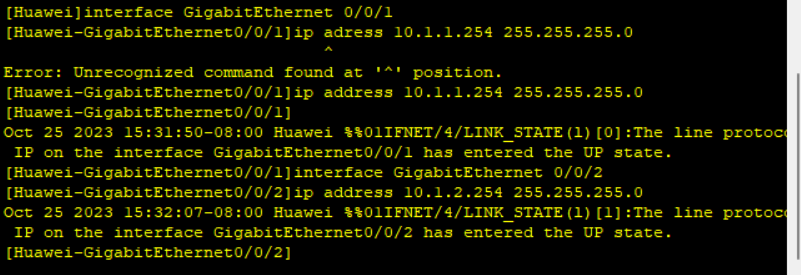
根据实验编址表进行相应的基本 IP 配置，并使用 ping 命令检测各链路的连通性

根据实验编址配置 PC 主机的 IP 地址及对应的掩码，掩码长度为 16。配置完成后，在命令行使用arp-a命令查看主机的 ARP 表

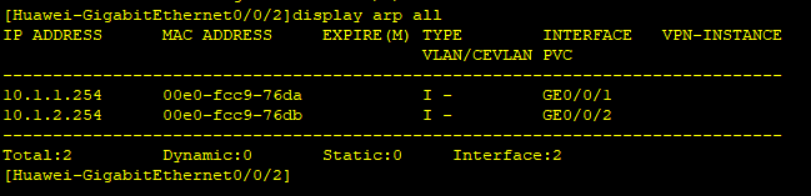


看到 ARP 表项为空，没有任何条目在里面

根据实验编址配置路由器 R1 的接口 IP 地址，掩码长度为 24。

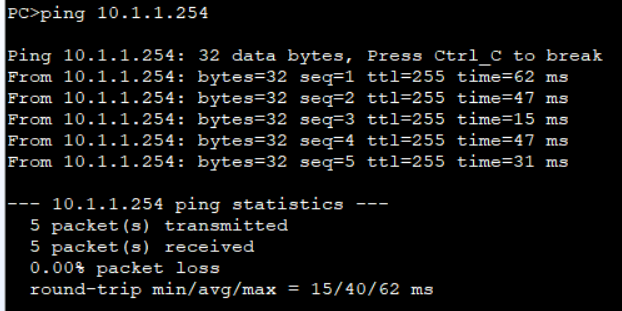


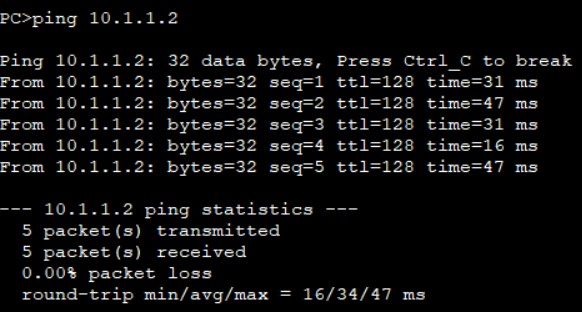
配置完成后，使用display arp all命令查看 R1 的 ARP 表



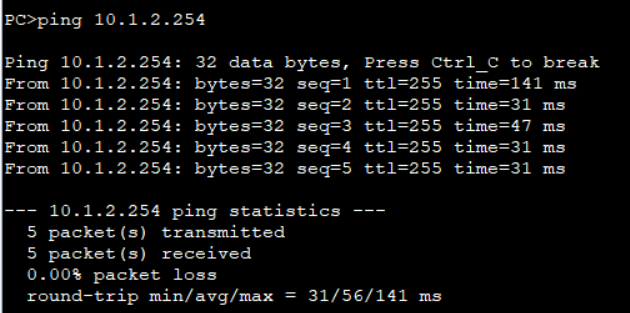
ARP 表中仅含有 R1 的两个接口 IP 地址及与其对应的 MAC 地址的 ARP 表项，没有其他条目

在 PC-1 上使用ping命令测试网关 R1 和 PC-2 的连通性





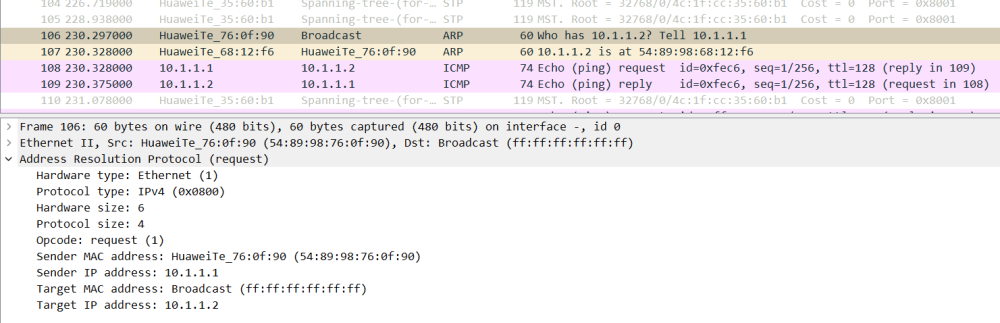
在 PC-3 上，使用ping命令测试到网关 R1 的连通性



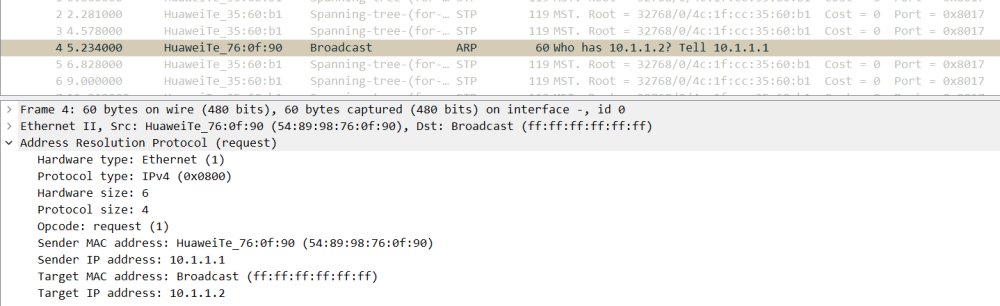
可以观察到直连网络连通性正常

当主机和网关之间有数据访问时，如果 ARP 表中没有目标IP地址与目标 MAC 地址的对应表项，ARP协议会被触发，向直连网段发送 ARP 广播请求包，请求目标 IP 地址所对应的 MAC 地址。

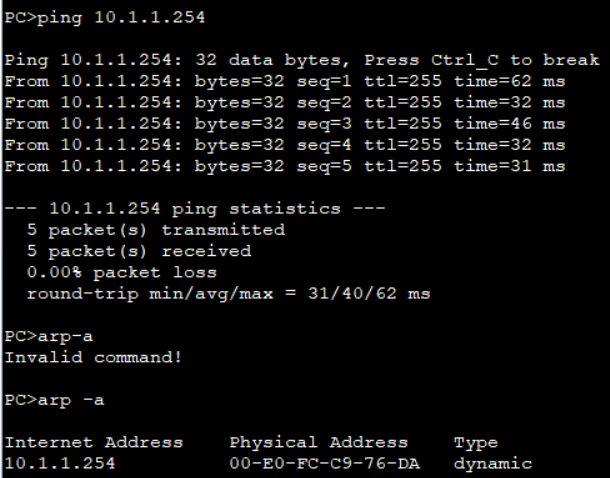
下图是 PC-1 发送的 ARP 广播请求，请求目标 IP 10.1.1.254 的 MAC 地址。

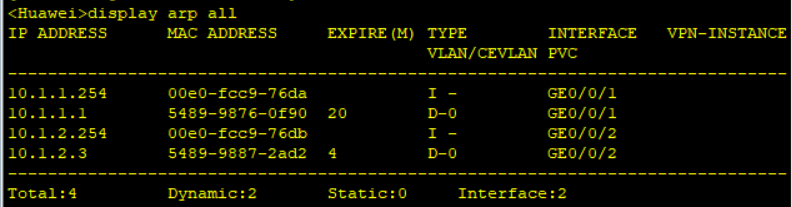


网关收到广播请求后，回应单播的 ARP 响应，里面含有自身往 IP 地址与 MAC 地址的对应关系



PC 和 R1 都会从这一对消息中知道对方的 IP 地址与 MAC 地址的对应关系，并将它写到各自的 ARP 表中。在 PC-1上ping网关 10.1.1.254 后，在 PC 上使用arp—a命令查看，在 R1 上使用display arp all命令查看。





可以观察到，在 PC-1 上生成了网关 IP 地址 10.1.1.254 和与其对应的 MAC 地址的 ARP 表项，在 R1 上生成了PC-1 的 IP 地址 10.1.1.1 和与其对应的 MAC 地址的 ARP 表项。上述出现在 PC 和 R1 里面的条目都是动态生成的。如果一段时间之后没有更新，便会从上述 ARP 表中删除。

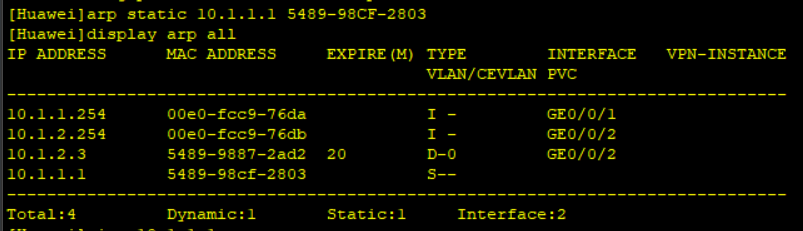
1. 配置静态 ARP

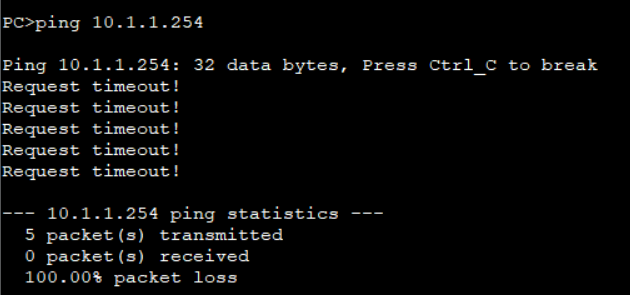
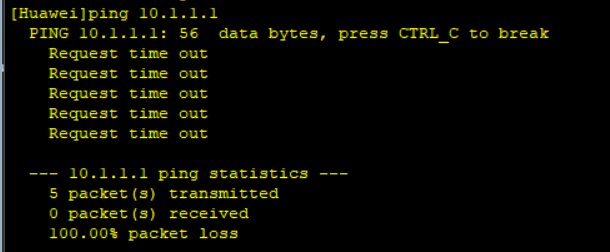
上述 ARP 协议的工作行为往往被攻击者利用。如果攻击者发送伪造的ARP报文，而且报文里面所通告的 IP 地址和MAC 地址的映射是错误的，则主机或网关会把错误的映射更新到 ARP 表中。当主机要发送数据到指定的目标IP地址时，从 ARP 表里得到了不正确的硬件 MAC 地址，并用之封装数据帧，导致数据帧无法正确发送。

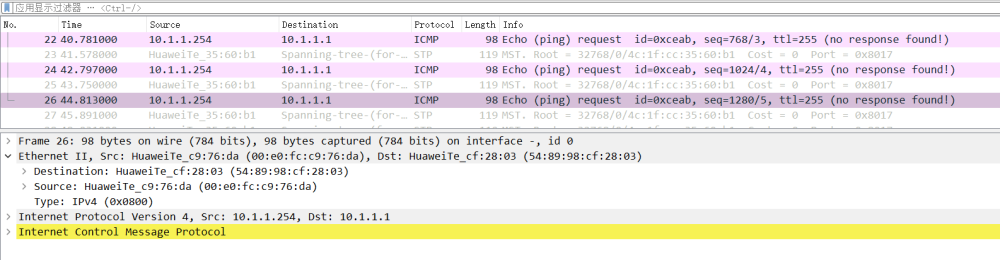
由于公司内主机感染了这种 ARP 病毒，所以主机对网关 R1 进行 ARP 攻击，向网关 R1 通告含错误映射的 ARP 通告，导致网关路由器上使用不正确的动态 ARP 映射条目，造成其他主机无法与网关正常通信。

模拟ARP攻击发生时，网络的通信受到了影响。在网关R1上，使用**arp static 10.1.1.1 5489-98CF-2803** 命令在路由器上静态添加一条关于 PC-1 的错误的 ARP 映射，假定此映射条目是通过一个 ARP 攻击报文所获得的（静态的条目优于动态的条目），所以错误的映射将出现在 ARP 表中。

使用**display arp all**命令查看 ARP 表，并使用 **ping**命令测试 PC-1 和网关之间的连通性

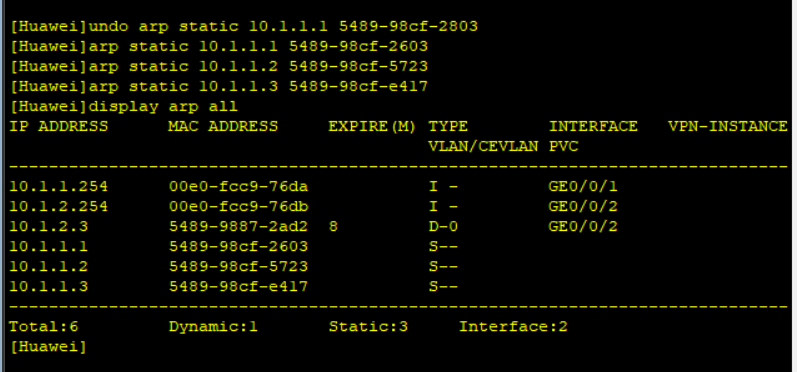




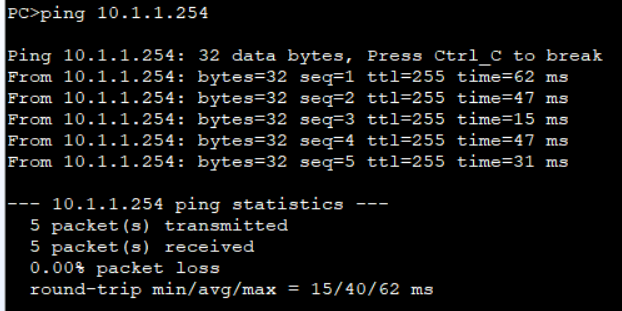
可以观察到，PC-1 与网关间无法通信，因为在路由器 R1 上 ARP 的映射错误，导致路由器无法正确地发送数据包给 PC-1。在 R1 的 GE 0/0/1 接口抓包观察

可以观察到，由于配置了静态 ARP ， R1 发往 PC-1 的 ping 包的二层头部，目的 MAC 地址被错误地封装为 5489-98CF-2803。

应对 ARP 欺骗攻击，防止其感染路由器的 ARP 表，可以通过配置静态 ARP 表项来实现。如果 IP 地址和一个 MAC 地址的静态映射已经出现在 ARP 表中，则通过动态 ARP 方式学来的映射则无法进入 ARP 表。所以针对公司网络的现状，网络管理员在 R1 上手工配置三条关于 PC-1、PC-2和PC-3 的正确 ARP 映射。使用arp static命令，配置如下。



配置完成后，在 PC-1 上测试

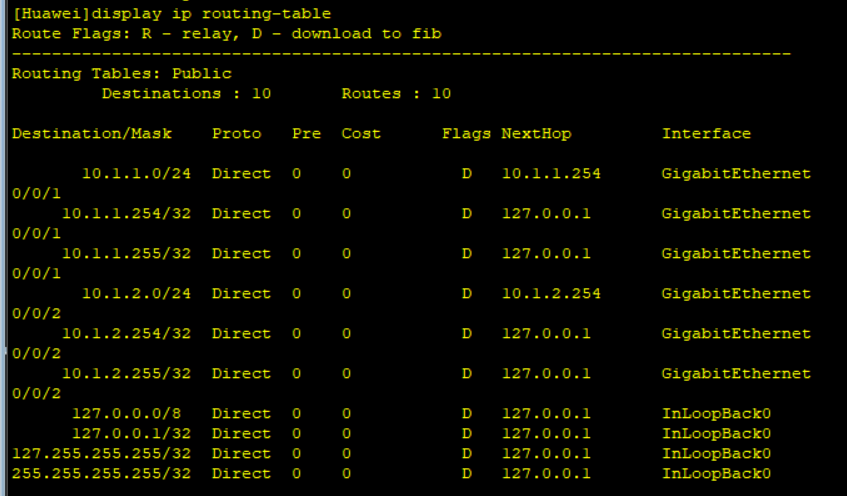


可以观察到，配置后连通性恢复正常。

公司网络中出现 ARP 攻击的情况是比较常见的，防御的办法之一是在 ARP 表中手工添加 ARP 映射。此种方法的优点是简单易操作，不足之处是网络中每个网络设备都有 ARP 表，要全方位保护网络就要在尽可能多的三层设备上把全网的 ARP 映射手工写入到 ARP 表里，工作量过大，如果更换 IP 或 MAC 后，还需要手工更新 ARP 映射，远没有动态 ARP 协议维护 ARP 表方便。但如果公司网络规模不大或者网络设备不多的情况 下，静态 ARP 方案还是具有一定优势的。

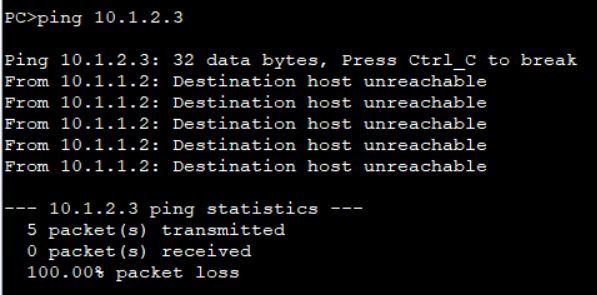
1. 配置 Proxy ARP

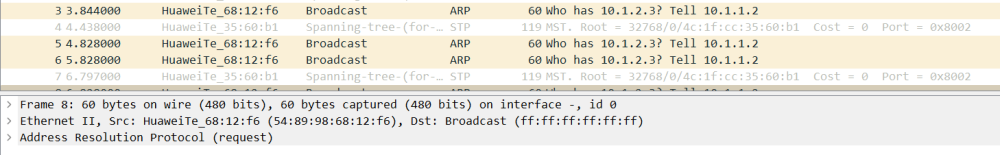
目前公司的网络被路由器 R1 分割为两个独立的广播域，每个路由器接口对应一个 IP 网络，分别是10.1.1.0/24和10/1/2/0/24，查看 R1 的路由表。



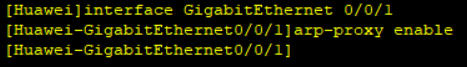
默认情况下，路由器上的 APR 代理功能是关闭的。

如果 R1 保持 ARP 代理功能关闭的情况，则 PC-2 和 PC-3 之间不能互相通信。在 PC-2 上，使用**ping**访问10.1.2.3，并在 PC-2 的 E 0/0/1 接口抓包来观察

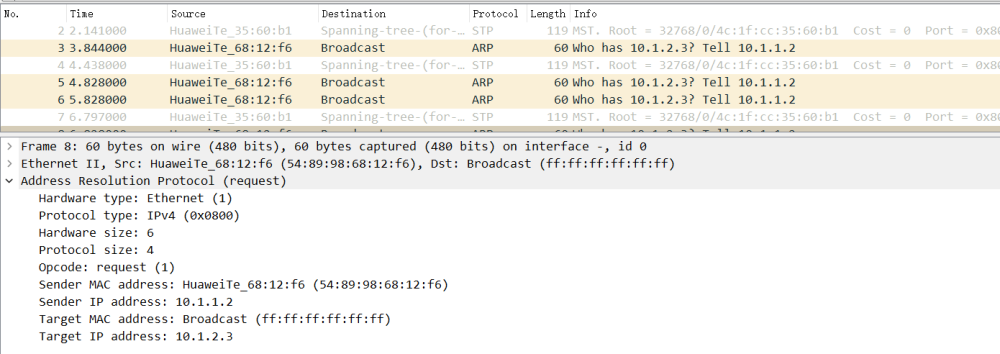




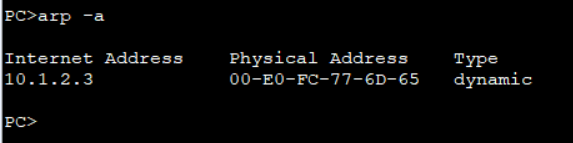
可以观察到，PC-2 发出了 ARP广播，却一直没有收到 ARP 响应。原因是 PC-2 和 PC-3 分处在两个广播域内， PC-2 发的ARP请求无法跨越中间的路由器，所以 PC-3 收不到 PC-2 的 ARP 请求，PC-2 也无法知晓目标主机PC-3 的硬件 MAC 地址而导致数据封装失败。但 R1 如果开启 ARP 代理之后，看是否能够解决这个问题。配置arp-proxy enable命令在路由器的接口上来开启 ARP 代理功能。



启用 ARP 代理之后，同样的测试，在 PC-2 上访问 PC-3 并在 PC-2 的 E 0/0/1 接口抓包观察

可以观察到，PC-2 发出了 ARP 请求并收到了 ARP 响应，但响应中10.1.2.3所对应 的硬件 MAC 地址并非是PC-3 的 MAC 地址，而是网关 R1 的 GE 0/0/1 接口 MAC 地址。

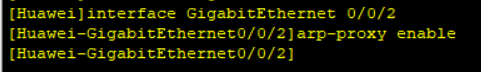
在PC-2上查看ARP表。



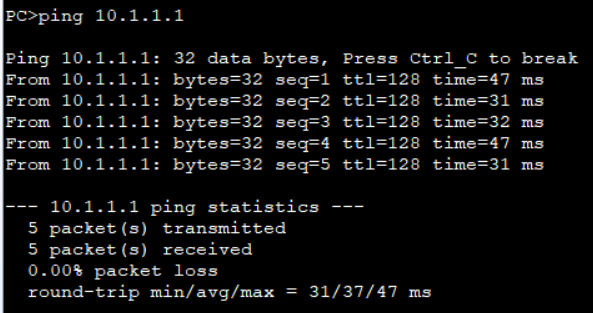
开启ARP代理后，PC-2 访问 PC-3 的工作过程如下。

R1的 接口 GE 0/0/1 开启了 ARP 代理后，收到 PC-2 的 ARP 广播请求报文后，R1 根据 ARP 请求中的目标IP地址10.1.2.3查看自身的路由表中是否有对应的目标网络， R1 的 GE 0/0/2 接口就是10.1.2.0/24网络，所以，R1 直接把自身的 GE 0/0/1 接口的 MAC 地址通过 ARP 响应返回给 PC-2, PC-2 接收到此 ARP 响应后横用该 MAC 作为目标硬件 地址发送报文给 R1, R1收到后再把报文转发给 PC-3。

同理，PC-3 要能访问R1连接的其他广播域的 PC,也需要在 R1 的 GE 0/0/2 接口上开启 ARP 代理功能。



配置完成后，测试PC-3与PC-1间的连通性。



可以观察到，通信正常。

如果IP网络过大，广播对网络的影响也相应增大.在不改变网络主机配置的情况 下，由管理员在网络中透明地插入一台路由器，靠路由器分割出多个广播域，降低了 广播对网络的影响。在当前的IP网络中，此种做法并不多见。其缺点是主机间的通信会因为引入额外的路由器而延迟增大，并存在着瓶颈问题，所以一般只作为临时解决方案使用。

### 五、讨论与分析

**思考**

**在ARP代理开启的情况下，如果在PC-2上，ping 10.1.2.4 (10.1.2.4主机不存在)，icmp echo报文是在 PC-2 还是 R1 路由器丢掉的？为什么？**

在ARP代理（ARP Proxy）开启的情况下，当PC-2尝试ping不存在的主机10.1.2.4时，icmp echo请求会被R1路由器丢弃。

因为ARP代理是一种机制，它允许一个设备（通常是路由器）代表另一个设备响应ARP请求。在这种情况下，如果PC-2尝试ping 10.1.2.4，它会发送一个ARP请求，询问10.1.2.4的MAC地址。由于10.1.2.4不存在，ARP请求将被R1路由器代理，R1将尝试回应ARP请求。但是R1不知道10.1.2.4不存在（因为它不在它的路由表中），所以R1将不会能够为10.1.2.4提供有效的MAC地址。在这种情况下，R1会丢弃PC-2发送的icmp echo请求，因为它无法为目标IP地址提供正确的下一跳。所以，icmp echo请求在R1路由器上被丢弃，因为R1是ARP代理，代表不存在的10.1.2.4尝试响应ARP请求，但无法提供有效的MAC地址。

**收获**

了解ARP的重要性和原理，以及它在网络通信中的作用，让我知道ARP协议是理解网络通信的基础。了解设备如何通过IP地址查找MAC地址，有助于深入了解网络通信的流程。

同时了解ARP欺骗是一种网络攻击方式，攻击者伪装成网络上的合法设备，通过篡改ARP表来进行中间人攻击。理解ARP欺骗有助于实施网络安全措施，如使用静态ARP表项或ARP检测工具来防范此类攻击。