

ARP协议仿真实验设计与实现

孙光懿

(天津音乐学院 网络安全和信息化办公室, 天津 300171)

摘要: ARP协议是TCP/IP协议栈中重要的协议之一,掌握其工作原理对于理解局域网底层通信逻辑至关重要。文章不仅分析了同网段通信时ARP协议的工作原理,而且还分析了跨网段通信时ARP协议的工作原理,并给出了相关仿真实验过程。研究对于更好地理解 and 掌握ARP协议,解决在现实中遇到的网络问题具有实践指导意义。

关键词: ARP; 以太网; 广播报文

中图分类号: TP393 **文献标识码:** A **文章编号:** 1008-9659(2024)03-0001-10

地址解析协议(Address Resolution Protocol, ARP)^[1]是OSI参考模型网络层中极其重要的协议。在以太网环境中,数据的传输基于MAC地址进行,而非IP地址。发送方不仅需要获取目标IP地址,而且还需要获取其MAC地址才能实现数据报文的传输。这是因为数据报文需要按照OSI参考模型从上至下进行封装^[2],直到封装到数据链路层以太网数据帧中才可对外发送,而构造以太网数据帧必须获取目标MAC地址。ARP协议的诞生完美解决了这一问题,它提供了一种由目标IP地址获取其MAC地址的机制,以确保数据报文的传输。

1 以太网帧结构

在实践中,以太网传输的数据帧有Ethernet II帧格式^[3]和IEEE802.3^[4]两种格式,具体使用哪种格式由网络层决定。二者之间的主要区别在于,Ethernet II帧格式存在一个2个字节的Type字段,而IEEE802.3格式字段的位置为长度字段。Ethernet II帧格式如图1所示,从图中可以发现,一是Ethernet II帧格式共有目的MAC地址(用来标识数据帧的接收方)、源MAC地址(用来标识数据帧的发送方)、类型、数据(用来标识IP数据包,其最大长度为1500字节,超过该字节数据包会被分片传输)、循环冗余校验(用来检测数据传输过程中的正确性和完整性)等五个字段;二是标准以太网环境中数据报文的传输,必须要获取接收方的MAC地址,才能将数据报文封装到MAC帧中,而只有ARP协议才具有根据接收方IP地址获取其MAC地址的能力。

6B	6B	2B	46-1500B	4B
D.MAC	S.MAC	Type	Data	FCS

图1 Ethernet II帧格式

2 ARP协议工作原理

2.1 ARP缓存表

为避免在传输数据报文时发送方频繁运行ARP协议,为提高传输效率,终端计算机、路由器等设备在运

[收稿日期]2024-01-18

[修回日期]2024-03-02

[基金项目]2023年天津市普通高等学校本科教学改革与质量建设研究计划项目(B231007201)。

[作者简介]孙光懿(1979-),男,高级工程师,主要从事计算机网络方面研究,E-mail:sunguangyi@tjcm.edu.cn.

行 ARP 协议时,通常会使用其缓存机制^[5],即 ARP 缓存表来存放近期解析出的 IP 地址和 MAC 地址映射条目。这样在传输数据报文时,发送方会先在自身 ARP 缓存表中查询目的 MAC 地址。若能查询成功,则直接将数据报文封装成以太网数据帧;若查询失败,则发送 ARP 请求广播报文。需要注意的是,ARP 缓存表不仅可以被查看、添加、修改(不同厂商相关命令有所不同),而且它还有生存时间,超过生存时间的映射条目将会从 ARP 缓存表中删除。

2.2 ARP 数据帧格式

ARP 数据帧^[5](有请求报文和 ARP 响应报文之分)总长共计 42 个字节。其中,以太网帧首部 14 个字节,ARP 报文体 28 个字节(图 2),相关字段功能如下:(1)以太网帧首部源地址和目的地址各占 6 个字节;(2)当以太网帧首部帧类型字段值为 0x806 时,表示上层运行的是 ARP 协议;(3)ARP 报文体硬件类型字段用来定义运行 ARP 协议的网络类型,当该字段值为“1”时,表示运行 ARP 协议的网络为以太网;(4)ARP 报文体协议类型字段用来定义上层使用的是哪种网络协议,当该字段值为“0800”时上层使用的是 IPv4 协议;(5)ARP 报文体硬件地址长度字段用来定义物理地址长度;(6)ARP 报文体逻辑地址长度字段用来定义逻辑地址长度;(7)当 ARP 报文体操作类型字段值为“1”时,表示为 ARP 请求报文;当操作类型字段值为“2”时,表示为 ARP 应答报文;(8)ARP 报文体发送端以太网地址字段用来定义发送 ARP 请求设备的 MAC 地址,该地址与以太网帧首部源地址相同;(9)ARP 报文体发送端 IP 地址字段用来定义发送 ARP 请求设备的 IP 地址;(10)ARP 报文体目的以太网地址和目的 IP 地址字段分别用来定义目的端设备 MAC 地址和 IP 地址。

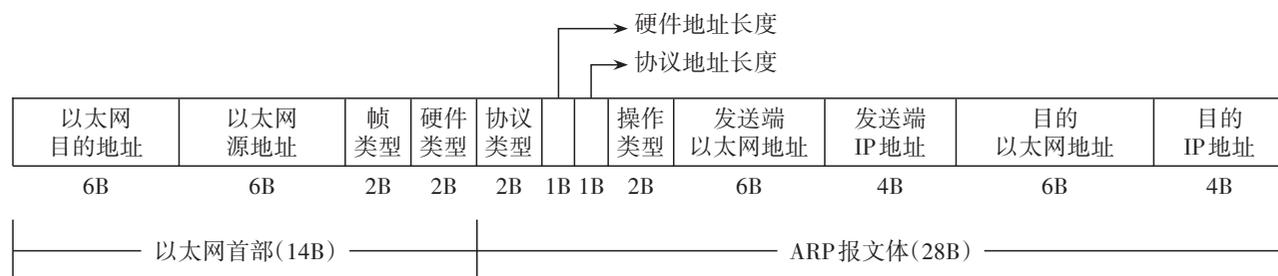


图2 ARP 数据帧格式

2.3 同网段通信时 ARP 协议工作原理

以主机 A 和主机 B 为例,当主机 A 向主机 B 发送数据报文时,首先会在自己的 ARP 缓存表中查询主机 B 的 IP 地址。若查询成功,则继续查询与其对应的 MAC 地址,并将该 MAC 地址封装成以太网数据帧^[6]。但也不排除主机 A 无法查询到主机 B 的 IP 地址的情况,多数是因为主机 A 刚加电启动(此时 ARP 缓存表为空),或主机 B 刚加入到网络。一旦出现这种情况,主机 A 第一时间会运行 ARP 协议,构造 ARP 请求报文(发送端 IP 地址和以太网地址分别为主机 A 的 IP 地址和 MAC 地址,目的 IP 地址为主机 B 的 IP 地址,目的以太网地址为 00-00-00-00-00-00)。其次,主机 A 会将该 ARP 请求报文封装成以太网数据帧(以太网帧首部源地址为主机 A 的 MAC 地址,目的地址为 FF-FF-FF-FF-FF-FF),并以广播方式对外发送。再次,待主机 B 收到该报文后,会检测报文目的 IP 地址是否与自身 IP 地址相一致。如果二者不一致,则丢弃该报文;若二者相一致,则主机 B 会将主机 A 的 MAC 地址和 IP 地址映射关系添加到自身 ARP 缓存表中,为未来与主机 A 通信做准备。接着主机 B 会以单播方式向主机 A 发送 ARP 响应报文,告诉主机 A 自身的 MAC 地址(发送端以太网地址和发送端 IP 地址分别为主机 B 的 MAC 地址和 IP 地址,目的 IP 地址和目的以太网地址分别为主机 A 的 IP 地址和 MAC 地址)。最后,主机 A 在获得主机 B 的 MAC 地址后,会将发往主机 B 的数据报文封装到以太网数据帧中。同时,将主机 B 的 IP 地址与 MAC 地址的映射关系添加到自身 ARP 缓存表中。主机 A 与主机 B 再次进行通信时,主机 A 直接查询自身 ARP 缓存表即可,无需再对外发送 ARP 广播报文。

2.4 跨网段通信时 ARP 协议工作原理

跨网段主机间通信过程比同网段主机间通信过程略复杂^[7]。以主机 A(IP 地址:192.168.3.2/24,网关地址:192.168.3.1)和主机 B(IP 地址:192.168.4.2/24,网关地址:192.168.4.1)为例,当主机 A 向主机 B 发送数据

报文时,首先会在自身 ARP 缓存表中查询主机 B 的 MAC 地址。若未查询成功,则第一时间判断主机 B 是否与自己同一网段内。若二者不在同一网段内,则构造 ARP 请求报文(请求网关 MAC 地址),并将其封装成 ARP 数据帧。此时,ARP 数据帧以太网帧首部源地址为主机 A 的 MAC 地址,目的地址为 FF-FF-FF-FF-FF-FF (即以广播方式对外发送 ARP 请求报文)。其次,网关在收到 ARP 请求报文后,若发现请求的是自己的 IP 地址,则会以单播方式向主机 A 发送 ARP 响应报文。主机 A 在获得网关 MAC 地址后,会将数据报文发送至网关(此时目的 IP 地址为主机 B 的 IP 地址,以太网帧首部目的 MAC 地址为网关 MAC 地址)。再次,网关收到数据报文后,会对主机 B 的 IP 地址进行检查。若发现目的 IP 地址与自身 IP 地址不在同一网段,则会通过路由表对数据报文进行路由转发。但在转发前,网关会查询自身 ARP 缓存表。若 ARP 缓存表中不存在主机 B 的 MAC 地址映射,网关则会发送 ARP 请求报文查询主机 B 的 MAC 地址。主机 B 收到 ARP 请求报文后,若发现请求的是自己的 IP 地址,则会以单播方式向网关发送 ARP 响应报文。最后,网关在收到主机 B 的 MAC 地址后,一是会将主机 B 的 IP 地址与 MAC 地址映射关系添加到自身 ARP 缓存表中,二是会将发往主机 B 的数据报文封装成以太网数据帧(此时发送端 IP 地址为主机 A 的 IP 地址,以太网帧首部源 MAC 地址为路由器相关转发接口 MAC 地址)。主机 B 收到该数据帧后进行处理,至此发送过程结束。

3 仿真实验

3.1 同网段通信时 ARP 协议工作原理仿真实验

3.1.1 仿真实验拓扑设计

本次仿真实验基于思科网络模拟器 Cisco Packet Tracer 8.1 搭建^[8],通过一台思科 2950 二层交换机和四台终端计算机,虚拟构建出一个小型局域网,终端计算机均工作在 VLAN2 网段。为更清楚地理解 ARP 协议在同网段通信时工作原理,首先将思科 2950 二层交换机 SW1 各端口工作模式设置为 ACCESS。其次,在交换机 SW1 中创建 VLAN2,并将其所有端口统一划分到 VLAN2 中。最后,设置四台终端计算机的 IP 地址和子网掩码,实现四台终端计算机之间可以正常通信。网络拓扑如图 3 所示,从图中可以清楚地看到,四台终端计算机 PC1、PC2、PC3、PC4 分别使用双绞线与思科 2950 二层交换机 SW1 的 f0/1 端口、f0/2 端口、f0/3 端口及 f0/4 端口相连。其中,终端计算机 PC1 的 IP 地址和子网掩码为 192.168.30.2/24,MAC 地址为 0001.6330.C143;终端计算机 PC2 的 IP 地址和子网掩码为 192.168.30.3/24,MAC 地址为 000C.856E.25EB;终端计算机 PC3 的 IP 地址和子网掩码为 192.168.30.4/24,MAC 地址为 000A.F381.CBE7;终端计算机 PC4 的 IP 地址和子网掩码为 192.168.30.5/24,MAC 地址为 0000.0CC2.9DD9。

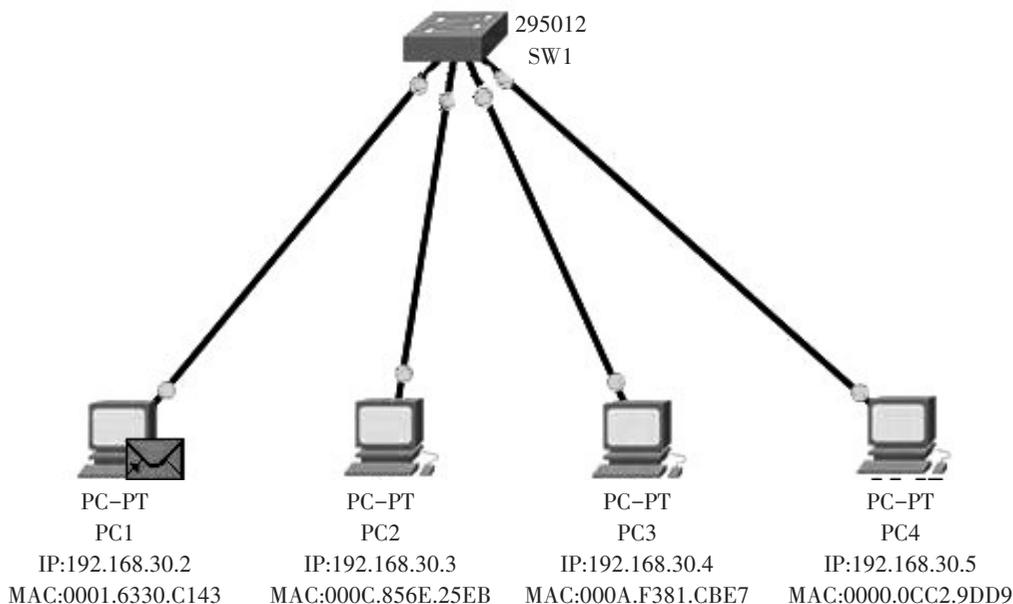


图3 ARP协议同网段通信仿真实验网络拓扑

3.1.2 仿真实验过程

仿真实验前,分别在四台终端计算机命令提示符界面输入“arp -a”命令,查看其 ARP 缓存表,结果发现上述各台终端计算机 ARP 缓存表均为空。在这里以终端计算机 PC1 为例(图4)。

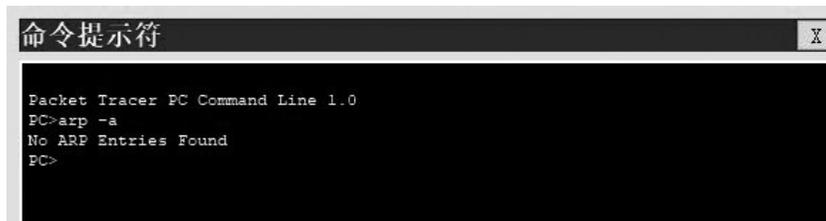


图4 仿真实验前终端计算机PC1中的ARP缓存表

为模拟同网段通信时 ARP 协议的工作原理,在终端计算机 PC1 上使用 PING 命令向终端计算机 PC3 发送 ICMP 数据包。终端计算机 PC1 会先检查自身 ARP 缓存表中是否存有终端计算机 PC3 的 MAC 地址信息。由于其 ARP 缓存表为空,因此终端计算机 PC1 以广播方式向全网发送 ARP 请求报文。具体仿真过程为:进入 Cisco Packet Tracer 网络模拟器选择模拟工作模式,并在该工作模式下点击编辑过滤器标签(注意只选择 ARP 协议)。而后进入终端计算机 PC1 的命令提示符界面输入“PING 192.168.30.4”命令,并确认回车(图5)。

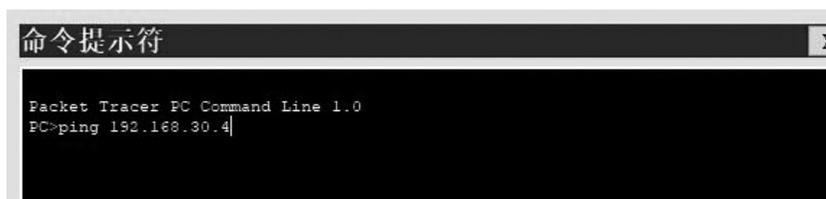


图5 使用PING命令向终端计算机PC3发送ICMP数据包

此时,终端计算机 PC1 的 ARP 请求报文正式生成。点击终端计算机 PC1 中的 Outbound PDU Details 标签查看 ARP 请求报文(图6)。由图6发现,一是在以太网帧首部中,源 MAC 地址为终端计算机 PC1 的 MAC 地址为 0001.6330.C143,目的 MAC 地址为 FF-FF-FF-FF-FF-FF,帧类型为“0x806”即网络层运行的是 ARP 协议;二是在 ARP 报文体中,协议类型为“0x800”,即 ARP 使用的是 IPv4 协议;操作类型字段为“0x1”,即该报文为 ARP 请求报文;源 MAC 地址和源 IP 地址分别为 0001.6330.C143 和 192.168.30.2,即终端计算机 PC1

设备 PC1 上的PDU信息

OSI Model Outbound PDU Details

PDU Formats

Ethernet II					
0	4	8	14	19	Bytes
前导码: 101010...1011		目的 MAC: FFFF.FFFF.FFFF		来源 MAC: 0001.6330.C143	
类型: 0x806	数据(可变长度)			帧校验序列: 0x0	

ARP				
0	8	16	31	Bits
硬件地址类型: 0x1		协议类型: 0x800		
HLEN: 0x6	PLEN: 0x4		OPCODE: 0x1	
SOURCE MAC: 0001.6330.C143 (48 bits)			SOURCE IP (32 bits) ==>	
192.168.30.2				
TARGET MAC: 0000.0000.0000 (48 bits)				
TARGET IP: 192.168.30.4 (32 bits)				

图6 终端计算机PC1发出的ARP请求报文

的 MAC 地址和 IP 地址;目的 IP 地址为 192.168.30.4,即终端计算机 PC3 的 IP 地址,目的 MAC 地址为 0000.0000.0000.

接下来点击 Capture/Forward 标签,模拟 ARP 报文的传输过程(图 7)。

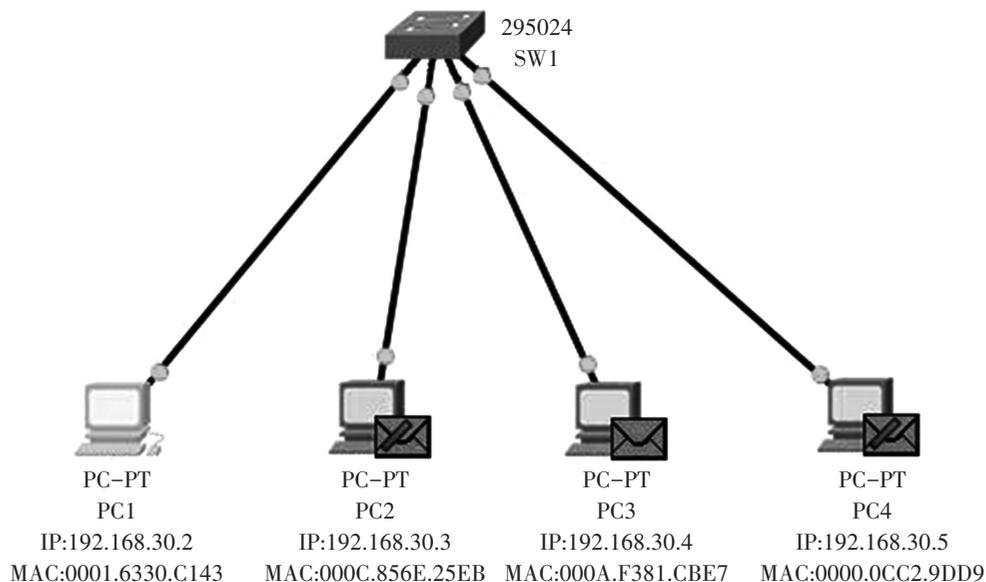


图 7 ARP 报文的传输过程

由图 7 发现,终端计算机 PC1 向全网进行 ARP 请求广播,局域网中其他终端计算机均收到了此 ARP 请求报文,但只有终端计算机 PC3 给予应答。根据同网段通信时 ARP 协议工作原理可知,此时 PC3 的 ARP 缓存表中已经记录了 PC1 的 IP 地址和 MAC 地址的映射关系,但终端计算机 PC1、PC2、PC3 的 ARP 缓存表依旧为空。在终端计算机 PC3 的命令提示符界面输入“arp-a”命令,查看 PC3 的 ARP 缓存表可以加以证实(图 8)。

```

命令提示符
Packet Tracer PC Command Line 1.0
PC>arp-a
Invalid Command.

PC>arp -a
Internet Address      Physical Address      Type
192.168.30.2         0001.6330.c143       dynamic
  
```

图 8 终端计算机 PC3 中的 ARP 缓存表

再点击终端计算机 PC3 中的 Outbound PDU Details 标签查看 ARP 应答报文^[9](图 9)。从图 9 中发现,一是在以太网帧首部中,源 MAC 地址为终端计算机 PC3 的 MAC 地址,为 000A.F381.CBE7,目的 MAC 地址为 0001.6330.C143,即终端计算机 PC1 的 MAC 地址;二是在 ARP 报文体中,操作类型字段为“0x2”,即该报文为 ARP 应答报文;源 MAC 地址和源 IP 地址分别为 000A.F381.CBE7 和 192.168.30.4,即终端计算机 PC3 的 MAC 地址和 IP 地址;目的 IP 地址为 192.168.30.2,即终端计算机 PC1 的 IP 地址;目的 MAC 地址为 0001.6330.C143,即终端计算机 PC1 的 MAC 地址。

再次点击 Capture/Forward 标签,继续模拟 ARP 报文的传输过程。当终端计算机 PC3 以单播方式发出的 ARP 应答报文到达终端计算机 PC1 时,PC1 的 ARP 缓存表会记录 PC3 的 IP 地址与 MAC 地址的映射关系(图 10)。

由图 10 发现,此次仿真实验结果与同网段通信时 ARP 协议工作原理分析结果相同。后续终端计算机 PC1 再访问终端计算机 PC3 时可直接从 ARP 缓存表中调用 PC3 的 MAC 地址进行数据帧封装^[10]。

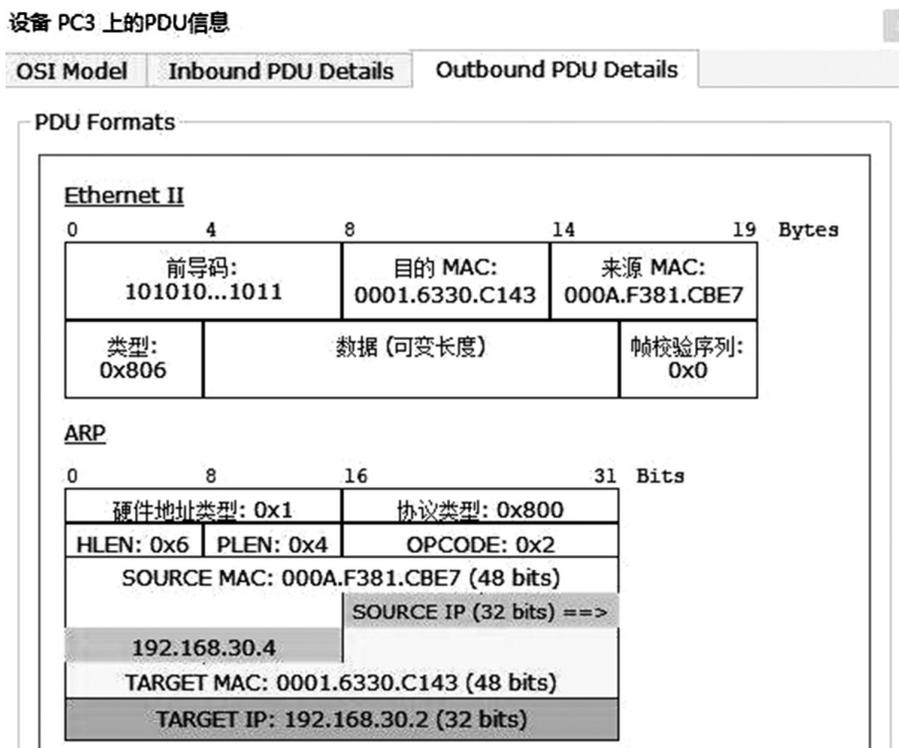


图9 终端计算机PC3发出的ARP应答报文

```

命令提示符
Packet Tracer PC Command Line 1.0
PC>ping
PC>ping 192.168.30.4

Pinging 192.168.30.4 with 32 bytes of data:

Reply from 192.168.30.4: bytes=32 time=8ms TTL=128
Reply from 192.168.30.4: bytes=32 time=4ms TTL=128
Reply from 192.168.30.4: bytes=32 time=4ms TTL=128
Reply from 192.168.30.4: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.30.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

PC>arp -a
Internet Address      Physical Address      Type
192.168.30.4          000a.f381.cbe7       dynamic

```

图10 收到ARP应答报文后终端计算机PC1中的ARP缓存表

3.2 跨网段通信时ARP协议工作原理仿真实验

3.2.1 仿真实验拓扑设计

本次仿真实验基于思科网络模拟器 Cisco Packet Tracer 8.1 搭建,通过两台思科 2960 交换机、一台思科 2911 路由器和四台终端计算机,虚拟构建出一个小型网络。其中,终端计算机 PC0、PC1 在 VLAN2 网段工作,PC2、PC3 在 VLAN3 网段工作。为更清楚地理解 ARP 协议在跨网段通信时的工作原理,首先将思科 2950 二层交换机 SW1、SW2 各端口工作模式设置为 ACCESS。其次,分别在交换机 SW1、SW2 中创建 VLAN2 和 VLAN3,并将 f0/1 ~ f0/10 端口和 f0/11 ~ f0/20 端口分别划分到 VLAN2 和 VLAN3 之中。网络拓扑如图 11 所示。从图中可以清楚地看到,路由器 Router1 的 G0/0 接口和 G0/1 接口分别与交换机 SW1、SW2 的 f0/3 端口相连,终端计算机 PC0、PC1 使用双绞线与思科 2960 交换机 SW1 的 f0/1 端口、f0/2 端口相连,终端计算机 PC2、PC3 使用双绞线与思科 2960 交换机 SW2 的 f0/11 端口、f0/12 端口相连。其中,路由器 Router1 的 G0/0 接口、

G0/1 接口的 IP 地址和子网掩码分别为 192.168.40.1/24 和 192.168.50.1/24, 终端计算机 PC0 的 IP 地址和子网掩码为 192.168.40.2/24, 网关地址为 192.168.40.1, MAC 地址为 0007.EC6C.81E2; 终端计算机 PC1 的 IP 地址和子网掩码为 192.168.40.3/24, 网关地址为 192.168.40.1, MAC 地址为 00D0.BC68.6927; 终端计算机 PC2 的 IP 地址和子网掩码为 192.168.50.2/24, 网关地址为 192.168.50.1, MAC 地址为 00E0.8F9D.1450; 终端计算机 PC3 的 IP 地址和子网掩码为 192.168.50.3/24, 网关地址为 192.168.50.1, MAC 地址为 00E0.F79C.0E83.

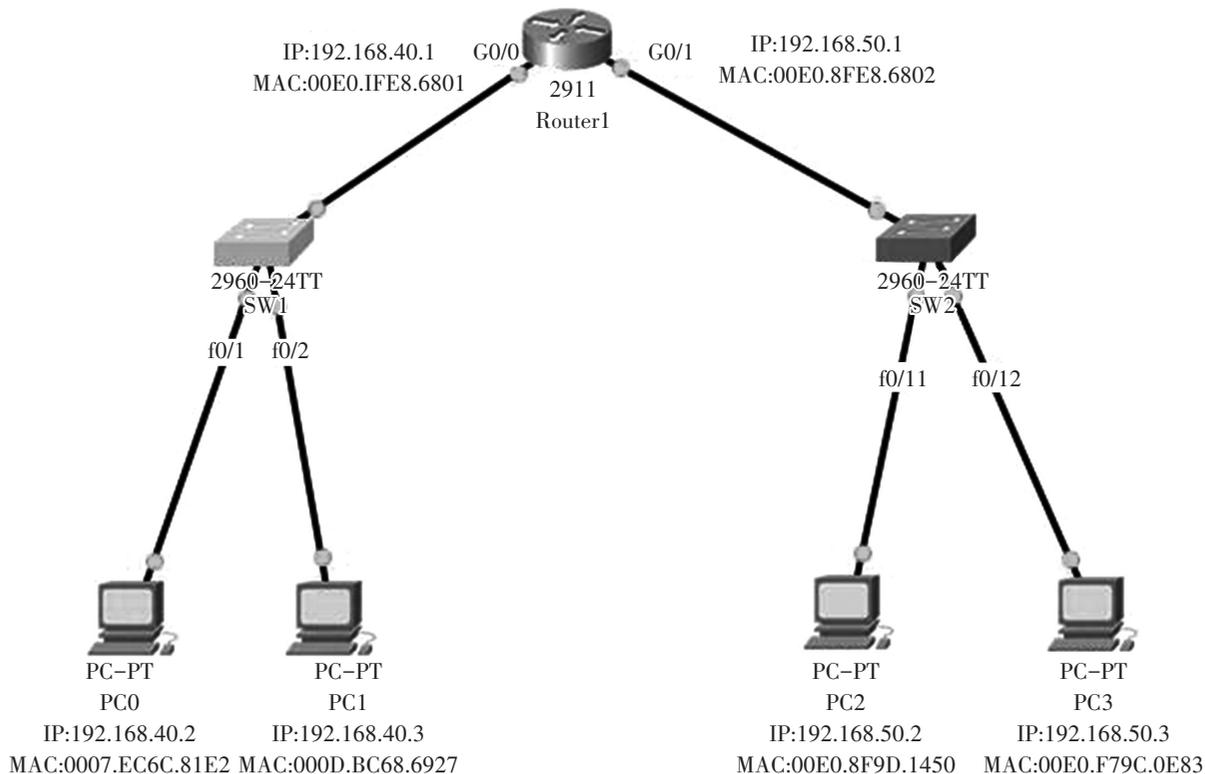


图 11 ARP 协议跨网段通信仿真实验网络拓扑

3.2.2 仿真实验过程

为模拟跨网段通信时 ARP 协议的工作原理, 在终端计算机 PC0 上使用 PING 命令向终端计算机 PC2 发送 ICMP 数据包。具体仿真实验过程为: 进入 Cisco Packet Tracer 网络模拟器选择模拟工作模式, 并在该工作模式下点击编辑过滤器标签。而后进入终端计算机 PC1 的命令提示符界面输入“PING 192.168.50.2”命令, 并确认回车。此时, 终端计算机 PC0 的 ARP 请求报文正式生成。

点击终端计算机 PC0 中的 Outbound PDU Details 标签查看 ARP 请求报文^[11](图 12)。从图中发现, 一是在以太网帧首部中, 源 MAC 地址为终端计算机 PC0 的 MAC 地址为 0007.EC6C.81E2, 目的 MAC 地址为 FF-FE-FE-FE-FE-FE, 帧类型为“0x806”即网络层运行的是 ARP 协议; 二是在 ARP 报文体中, 协议类型为“0x800”, 即 ARP 使用的是 IPv4 协议; 操作类型字段为“0x1”, 即该报文为 ARP 请求报文, 源 MAC 地址和源 IP 地址分别为 0007.EC6C.81E2 和 192.168.40.2, 即终端计算机 PC0 的 MAC 地址和 IP 地址, 目的 IP 地址为 192.168.40.1, 即终端计算机 PC0 的网关地址, 目的 MAC 地址为 0000.0000.0000。

接下来通过点击 Capture/Forward 标签, 模拟 ARP 请求报文的传输过程^[12](图 13)。从图中发现, 终端计算机 PC1 和路由器 Router1 的 G0/0 接口均收到了该 ARP 请求报文, 但只有路由器 Router1 的 G0/0 接口给予应答。

根据跨网段通信时 ARP 协议工作原理分析可知, 此时路由器 Router1 的 ARP 缓存表已经记录了终端计算机 PC0 的 IP 地址和 MAC 地址的映射关系, 但终端计算机 PC0、PC1、PC2、PC3 的 ARP 缓存表依旧为空。在路由器 Router1 的 CLI 界面输入“sh arp”命令, 查看路由器 Router1 的 ARP 缓存表可以证实(图 14)。

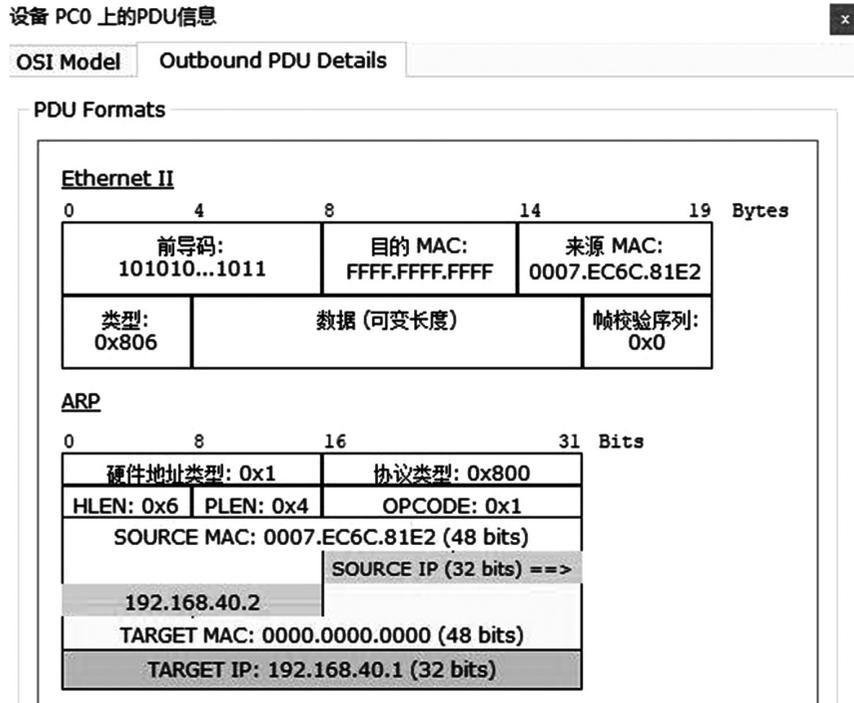


图 12 终端计算机 PC0 发出的 ARP 请求报文

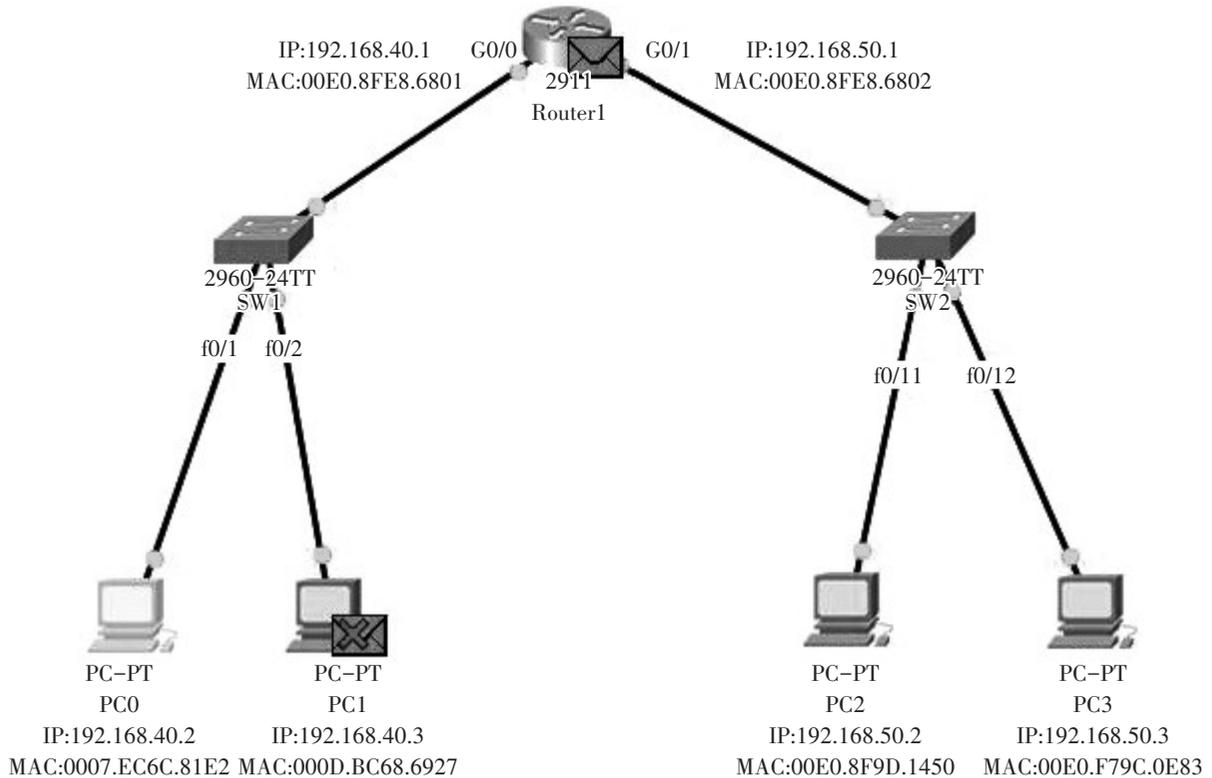


图 13 跨网段通信时 ARP 报文的传输过程

```

Router1#sh arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.40.1 - 00E0.8FE8.6801 ARPA GigabitEthernet0/0
Internet 192.168.40.2 0 0007.EC6C.81E2 ARPA GigabitEthernet0/0
Internet 192.168.50.1 - 00E0.8FE8.6802 ARPA GigabitEthernet0/1
    
```

图 14 路由器 Router1 的 ARP 缓存表

再点击路由器 Router1 中的 Outbound PDU Details 标签查看 ARP 应答报文(图 15)。从图中发现,一是在以太网帧首部中,源 MAC 地址为路由器 Router1 G0/0 接口的 MAC 地址,为 00E0.8FE8.6801,目的 MAC 地址为 0007.EC6C.81E2,即终端计算机 PC0 的 MAC 地址;二是在 ARP 报文体中,操作类型字段为“0x2”,即该报文为 ARP 应答报文;源 MAC 地址和源 IP 地址分别为 00E0.8FE8.6801 和 192.168.40.1,即路由器 Router1 G0/0 接口的 MAC 地址和 IP 地址,目的 IP 地址为 192.168.40.2,即终端计算机 PC0 的 IP 地址,目的 MAC 地址为 0007.EC6C.81E2,即终端计算机 PC0 的 MAC 地址。

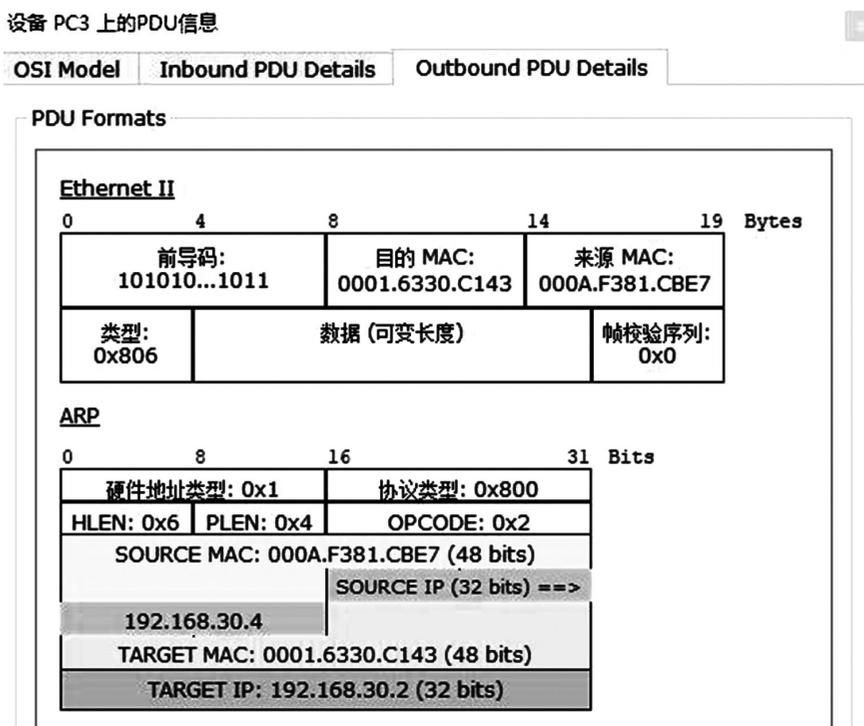


图 15 路由器 Router1 发出的 ARP 应答报文

再次点击 Capture/Forward 标签,继续模拟 ARP 应答报文的传输过程^[13-14]。当路由器 Router1 以单播方式发出的 ARP 应答报文到达终端计算机 PC0 时,PC0 的 ARP 缓存表会记录网关 IP 地址与 MAC 地址的映射关系(图 16)。从图中发现,此次仿真实验结果与跨网段通信时 ARP 协议工作原理分析结果相同。后续终端计算机 PC0 再访问 VLAN3 网段所属终端计算机时可直接从 ARP 缓存表中调用网关 MAC 地址进行数据帧封装。待数据帧到达路由器 Router1 后,路由器 Router1 会根据路由表进行转发^[15],继续进行 ARP 协议工作过程,直到路由器 Router1 能够获取终端计算机 PC2 的 MAC 地址。

```
PC>arp -a
Internet Address      Physical Address      Type
192.168.40.1         00e0.8fe8.6801      dynamic
```

图 16 收到 ARP 应答报文后终端计算机 PC0 中的 ARP 缓存表

4 结语

通过研究可知,ARP 协议可根据目标 IP 地址解析出目标 MAC 地址,实现数据包由网络层到数据链路层的封装和转发。文章设计了 ARP 协议工作原理仿真实验,并利用思科网络模拟器 Cisco Packet Tracer 模拟了 ARP 协议在同网段通信时的工作过程和跨网段通信时的工作过程,最终实验结果与理论分析结果相一致。此举不仅有助于读者对 ARP 协议工作原理有一个全新的认识,而且还有助于达到理论与实验相互促进的效果。

参考文献:

- [1] BALAJI S. CCNP SWITCH学习指南[M].北京:人民邮电出版社,2011.
- [2] 孙光懿.国内院校IPv6应用生态建设路径研究[J].首都师范大学学报(自然科学版),2023,44(02):11-14.
- [3] 冯昊,黄治虎,伍技祥.交换机/路由器配置与管理[M].北京:清华大学出版社,2010.
- [4] 张雪梅.国产化某OS中IP协议族的研究与应用[D].西安:西安工业大学,2021.
- [5] 杨妹,罗佳.基于Packet Tracer软件的小型局域网设计与仿真[J].实验技术与管理,2015,32(01):150-152.
- [6] 马素刚,赵婧如,孙韩林.计算机组网实验教程[M].西安:西安电子科技大学出版社,2014.
- [7] 张莉.高校机房ARP欺骗攻击的解决方案[J].山西财经大学学报,2013,35(S2):89.
- [8] 唐灯平,王进,肖广娣.ARP协议原理仿真实验的设计与实现[J].实验室研究与探索,2016,35(12):126-129,196.
- [9] 赵梦娜.基于校园网的ARP攻击系统的设计与实现[D].广州:华南理工大学,2013.
- [10] 洪新建,洪新华.一种基于验证机制的ARP协议改进算法[J].计算机安全,2014,(04):22-24.
- [11] 史隽彬,秦科.ARP攻击现状分析及一种应对ARP攻击的方法[J].陕西理工学院学报(自然科学版),2013,29(02):45-49.
- [12] 张钢,黄小波.思科虚拟实验平台的构建[J].实验室研究与探索,2010,(08):216-218.
- [13] 徐济成,朱昊,李静月.基于VRRP的网络鲁棒性研究[J].重庆文理学院学报,2015,34(02):95-98.
- [14] 张钢.思科虚拟实验平台的构建[J].实验室研究与探索,2010,(08):216-218.
- [15] 王文彦.计算机网络实践教程[M].北京:人民邮电出版社,2014.

Design and Implementation of ARP Protocol Simulation Experiment

SUN Guang-yi

*(Office of Network Security and Information Technology, Tianjin Conservatory of Music,
Tianjin, 300171, China)*

Abstract: The ARP protocol is one of the important protocols in the TCP/IP protocol stack, and mastering its working principle is crucial for understanding the communication logic of Ethernet. This article not only analyzes the working principle of the ARP protocol when communicating with the same network segments, but also analyzes the working principle of the ARP protocol when communicating across network segments, and provides relevant simulation experiments. This research has practical significance for better understanding and mastering the ARP protocol, and solving network problems encountered in reality.

Keywords: ARP; Ethernet; Broadcast