网络编程基础

ARP：网络世界到物理世界的桥梁

目录

RT-Thread

简介

简介

- ARP（Address Resolution Protocol）地址解析协议，是根据 IP 地址获取物理 MAC 地址的一个 TCP/IP 协议。

- 现在局域网中主机的 IP 一般都是动态分配的，这样做的好处是提高了 IP 的利用率；缺点是，当数据到来时只根据 IP 地址就不能确定到底哪一台主机了。因此需要弄一个缓存表，用来记录 IP 和 主机 MAC 地址的对应关系，这个缓存表就是 ARP 高速缓冲表 。

- ARP协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，同时，维护 ARP 高速缓冲表，以保证通信的顺利进行。

协议解析

ARP 的分组格式

- 以太网的源地址和目的地址：目的地址为全 1 的特殊地址是广播地址。电缆上的所有以太网接口都要接收广播的数据帧。
- 帧类型：表示后面数据的类型。对于 ARP 请求或应答来说，该字段的值为 0x0806。
- 硬件类型：表示硬件地址的类型。它的值为 1 即表示以太网地址。

RT-Thread

ARP 的分组格式

- 协议类型：表示要映射的协议地址类型。它的值为 0x0800 即表示 IPv4 协议。
- 硬件地址长度和协议地址长度：分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 4 和 6。
- 操作字段：指出四种操作类型，它们是 ARP 请求（值为1）、ARP 应答（值为2）、RARP 请求（值为3）和 RARP 应答（值为 4）。

ARP 过程分析

ARP 过程分析

例如：

- 主机 A ： IP：192.168.0.2；MAC：00-00-C0-15-AD-18.
- 主机 B ： IP：192.168.0.4；MAC：08-00-2B-00-EE-AA.

当局域网的主机 A 接收到发给 IP：192.168.0.4 的数据，他就需要转发数据给主机 B，首先主机 A先查询自己的 ARP 缓存看是否有与此 IP 对应的 MAC 地址，如果没有的话，主机 A 就会运行 ARP。

- 主机 A 在本局域网广播一个 ARP 请求分组 。ARP请求分组的主要内容是表明：我的 IP 地址是 192.168.0.2，我的 MAC 地址是 00-00-C0-15-AD-18 .我想知道 IP 地址为 192.168.0.4 的主机的 MAC 地址。
- 在本局域网上的所有主机都收到此 ARP 请求分组。

ARP 过程分析

- 主机 B 在 ARP 请求分组中见到自己的 IP 地址，就向主机 A 发送 ARP 响应分组，并写入自己的 MAC 地址。其余的所有主机都不理睬这个 ARP 请求分组。ARP 响应分组的主要内容是表明：“我的 IP 地址是192.168.0.4,我的硬件地址是 08-00-2B-00-EE-AA ”,请注意：虽然 ARP 请求分组是广播发送的，但 ARP 响应分组是普通的单播，即从一个源地址发送到一个目的地址。
- 主机 A 收到主机 B 的 ARP 响应分组后，就在其 ARP 高速缓冲表中写入主机 B 的 IP 地址到 MAC 地址的映射。
- 然后，现在主机 A 就可以给主机 B 发送数据了。

工作流程

- 正常的工作流程如下：

抓包分析

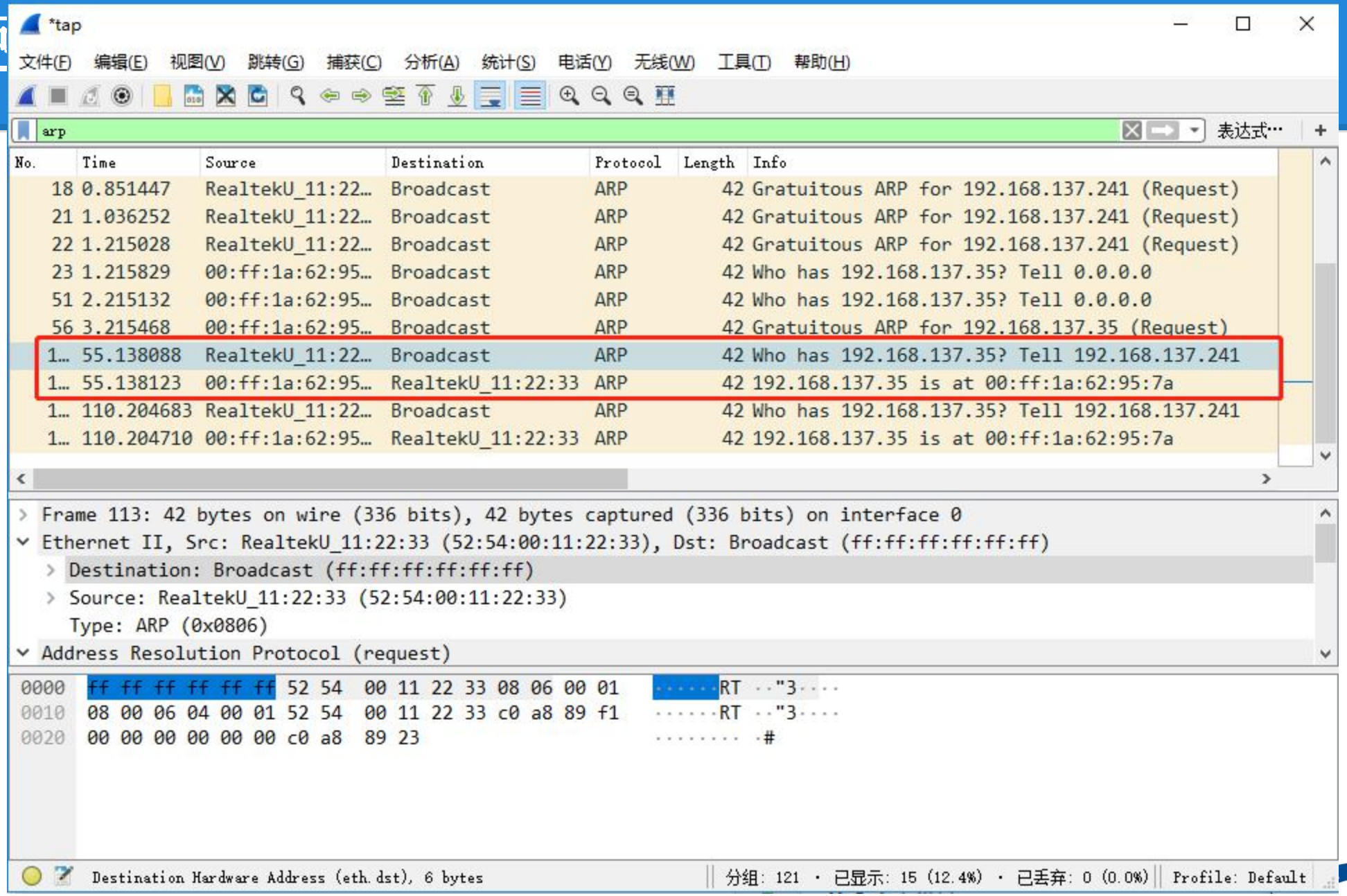
抓包分析

其实 QEMU 在刚开始运行的时候就会自动运行 ARP，只要在开始运行 QEMU 之前开启抓包就能抓到 ARP的包

1. 打开 wireshark 软件 开启抓包，设定过滤条件为 arp，只显示 ARP 协议的包。
2. 运行 QEMU

查看 wireshark ，发现已经抓到了 ARP 协议 的数据包

抓包


*tap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
arp
表达式…
No. Time Source Destination Protocol Length Info
18 0.851447 RealtekU_11:22… Broadcast ARP 42 Gratuitous ARP for 192.168.137.241 (Request)
21 1.036252 RealtekU_11:22… Broadcast ARP 42 Gratuitous ARP for 192.168.137.241 (Request)
22 1.215028 RealtekU_11:22… Broadcast ARP 42 Gratuitous ARP for 192.168.137.241 (Request)
23 1.215829 00:ff:1a:62:95… Broadcast ARP 42 Who has 192.168.137.35? Tell 0.0.0.0
51 2.215132 00:ff:1a:62:95… Broadcast ARP 42 Who has 192.168.137.35? Tell 0.0.0.0
56 3.215468 00:ff:1a:62:95… Broadcast ARP 42 Gratuitous ARP for 192.168.137.35 (Request)
1… 55.138088 RealtekU_11:22… Broadcast ARP 42 Who has 192.168.137.35? Tell 192.168.137.241
1… 55.138123 00:ff:1a:62:95… RealtekU_11:22:33 ARP 42 192.168.137.35 is at 00:ff:1a:62:95:7a
1… 110.204683 RealtekU_11:22… Broadcast ARP 42 Who has 192.168.137.35? Tell 192.168.137.241
1… 110.204710 00:ff:1a:62:95… RealtekU_11:22:33 ARP 42 192.168.137.35 is at 00:ff:1a:62:95:7a
Frame 113: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: RealtekU_11:22:33 (52:54:00:11:22:33), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: RealtekU_11:22:33 (52:54:00:11:22:33)
Type: ARP (0x0806)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 52 54 00 11 22 33 08 06 00 01
0010 08 00 06 04 00 01 52 54 00 11 22 33 c0 a8 89 f1
0020 00 00 00 00 00 00 c0 a8 89 23
Destination Hardware Address (eth.dst), 6 bytes
分组: 121 · 已显示: 15 (12.4%) · 已丢弃: 0 (0.0%)
Profile: Default

RT-Thread

抓包分析

- 我们也可以点开封包详细信息然后和上面的 ARP 的分组格式做对比

RT-Thread

抓包分析

- 当然还有回复 ARP 请求分组的数据包，如下图所示：

- 其他的一些选项对照着前面的报文格式做对比，就可以很容易的了解 ARP 协议的工作过程了。

RT-Thread