博客园 首页 新随笔 联系 管理 订阅 随笔- 8 文章- 0 评论- 1

山野樵夫

< 2014年8月 >

日	一	二	三	四	五	六
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

昵称：山野樵夫
园龄：1年11个月
粉丝：2
关注：2
+加关注

搜索

找找看

谷歌搜索

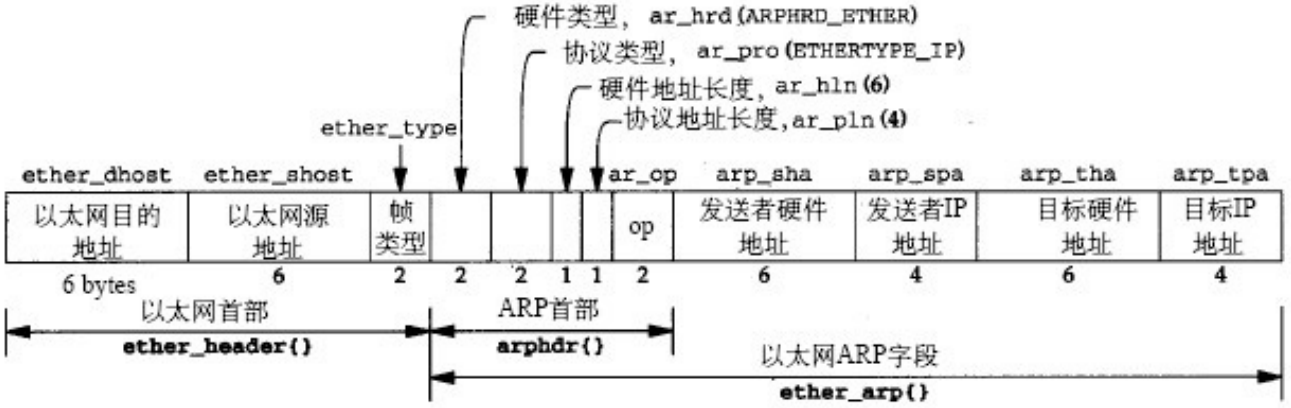
常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签
更多链接

我的标签

设计模式(3)
网络协议(1)
linux学习笔记(1)
Python(1)
编程基础(1)

ARP报文格式解析



首先，可以看到ARP报文是由14位的以太网首部和28位的ARP请求/应答构成的。来分析一下抓到的包：

阶乘问题(1)

随笔分类

设计模式(1)

随笔档案

2013年8月 (1)
2013年5月 (1)
2012年10月 (2)
2012年9月 (1)
2012年8月 (3)

阅读排行榜

1. ARP报文格式解析(246)
2. linux学习笔记(一)---正则表达式(45)
3. memcpy/memmove实现(34)
4. Python实例---发邮件(31)
5. N!末尾有多少个0(24)

评论排行榜

1. N!末尾有多少个0(1)

```
⊞ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊟ Ethernet II, Src: Hewlett-_c9:c0:1c (98:4b:e1:c9:c0:1c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊟ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ⊟ Source: Hewlett-_c9:c0:1c (98:4b:e1:c9:c0:1c)
      Address: Hewlett-_c9:c0:1c (98:4b:e1:c9:c0:1c)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Hewlett-_c9:c0:1c (98:4b:e1:c9:c0:1c)
    Sender IP address: 192.168.7.84 (192.168.7.84)
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.7.254 (192.168.7.254)

0000  ff ff ff ff ff ff 98 4b  e1 c9 c0 1c 08 06 00 01   .......K ........
0010  08 00 06 04 00 01 98 4b  e1 c9 c0 1c c0 a8 07 54   .......K .......T
0020  ff ff ff ff ff ff c0 a8  07 fe 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

我们按顺序来看，首先看以太网首部：

目的MAC地址,0xFF-FF-FF-FF-FF-FF,这是一个广播地址,目标是网络上所有的主机。

源MAC地址,这是请求端(发送端)的MAC地址。

协议类型,表明以太网帧的类型,这里是0x0806,代表这是ARP协议帧。

然后来看ARP报文：

硬件类型,1代表是以太网。

协议类型,表明上层协议的类型,这里是0x0800,表示上层协议是IP协议

硬件地址长度,毫无疑问是6个字节

协议长度,这里IP协议的长度是4个字节

操作类型,在报文中占2个字节,1表示ARP请求,2表示ARP应答,3表示RARP请求,4表示RARP应答

发送方(源)MAC地址

发送方(源)IP地址

目的MAC地址

目的IP地址

ARP应答包与请求包不同之处在于,应答包中的源MAC地址是请求包中的目的MAC地址,目的MAC地址是请求包中的源MAC地址。以太网目的地址和源地址同理。

未完待续....

标签: 网络协议

绿色通道： 好文要顶 关注我 收藏该文 与我联系

山野樵夫
关注 - 2
粉丝 - 2
+加关注

0 0

(请您对文章做出评价)

« 上一篇：Python实例---发邮件

posted @ 2013-08-22 23:50 山野樵夫 阅读(245) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册，访问网站首页。

博客园首页 博问 新闻 闪存 程序员招聘 知识库

最新IT新闻:
· 极客爱情之十一：和不会聊天的人谈恋爱
· 从阿北的公开信，看豆瓣发生了什么，以及豆瓣将发生什么
· 摄影师发明水藻照片冲印法
· 2014《国家地理》摄影大赛中国区优秀作品
· 传说中的腾讯离职员工薪酬大曝光
» 更多新闻...

最新知识库文章:
· 父子页面之间跨域通信的方法
· Android开发在路上：少去踩坑，多走捷径
· 从用户行为打造活动交互设计闭环——2014年世界杯竞猜活动设计总结
· 如何通过一个问题，完成最成功的技术面试
· 我所理解的技术领导力
» 更多知识库文章...

Copyright ©2014 山野樵夫