

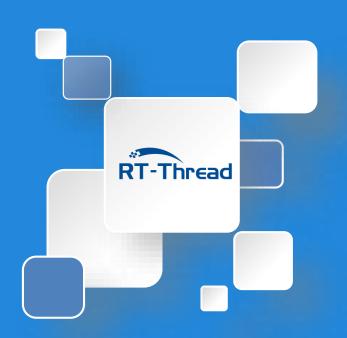
网络编程基础

一次完整的 Ping 过程

目录

- 抓一个 Ping 包
- 什么是 Ping
- Ping 包分析
- Ping 的过程





抓一个Ping包

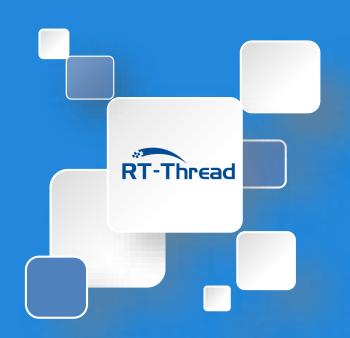
抓包分析

我们在用 wireshark 抓包的时候,用开发板 ping 一下百度 ,就可以抓到 Ping 的数据包了。

- 1. 打开 wireshark 软件开启抓包
- 2. 当 QEMU 连接上网络后,输入 ping <u>www.baidu.com</u>
- 3. 设定过滤条件,只显示和开发板 IP 相关的包

```
10 2.463950
             192.168.137.31
                              192.168.137.1
                                                            73 Standard query 0x56a7 A www.baidu.com
                                                DNS
                                                           132 Standard query response 0x56a7 A www.baidu.com CNAME www.a.shifen.
11 2.466730
             192.168.137.1
                              192.168.137.31
                                                DNS
                                                            74 Echo (ping) request id=0xafaf, seq=1/256, ttl=255 (reply in 13)
12 2.467707
             192.168.137.31
                                                ICMP
                              111.13.100.92
13 2.493058
             111.13.100.92
                              192.168.137.31
                                                ICMP
                                                            74 Echo (ping) reply id=0xafaf, seq=1/256, ttl=54 (request in 12)
14 2.671856
             192.168.137.31
                              111.13.100.92
                                                ICMP
                                                            74 Echo (ping) request id=0xafaf, seq=2/512, ttl=255 (reply in 15)
15 2.695936
             111.13.100.92
                              192.168.137.31
                                                ICMP
                                                            74 Echo (ping) reply id=0xafaf, seq=2/512, ttl=54 (request in 14)
16 2.880493
             192.168.137.31
                              111.13.100.92
                                                ICMP
                                                            74 Echo (ping) request id=0xafaf, seq=3/768, ttl=255 (reply in 17)
                                                ICMP
                                                            74 Echo (ping) reply id=0xafaf, seq=3/768, ttl=54 (request in 16)
17 2.904663
             111.13.100.92
                              192.168.137.31
                                                ICMP
                                                            74 Echo (ping) request id=0xafaf, seq=4/1024, ttl=255 (reply in 19)
18 3.093709
             192.168.137.31
                              111.13.100.92
19 3.117905
                                                            74 Echo (ping) reply
                                                                                   id=0xafaf, seq=4/1024, ttl=54 (request in 18)
             111.13.100.92
                              192.168.137.31
                                                ICMP
```





什么是Ping

Ping 简介

• 当我们要检查网络状况的时候,就总喜欢 Ping 一下百度,检测网络到底通不通。但是这一个看似简单的命令 Ping,到底涉及了什么协议,数据又经历了什么样的路程,今天我们就来看一看。



Ping 简介

- Ping 程序是用来探测主机到主机之间是否可通信,如果不能 Ping 到某台主机,表明不能和这台主机建立连接。
- Ping 使用的是 ICMP 协议,它发送 ICMP 回送请求消息给目的主机。ICMP 协议规定:目的主机必须返回 ICMP 回送应答消息给源主机。如果源主机在一定时间内收到应答,则认为主机可达。
- 一次完整的 Ping 过程其实涉及很多协议,如 <u>DNS</u>,<u>UDP</u>,<u>ARP</u>,<u>ICMP</u> 以及 <u>路由协议</u>等。



DNS

- DNS(Domain Name System,域名系统),万维网上作为域名(网址)和 IP 地址相互映射的一个分布式数据库,能够使用户更方便的访问互联网,而不用去记那一串毫无意义的数字组成的 IP 地址。
- 通过域名得到该域名对应的 IP 地址的过程叫做域名解析(或主机名解析)。 DNS 协议运行在 UDP 协议之上,使用端口号 53。
- 如果我们要 ping www.baidu.com 首先就要先进行 DNS 域名解析获得 IP 地址。



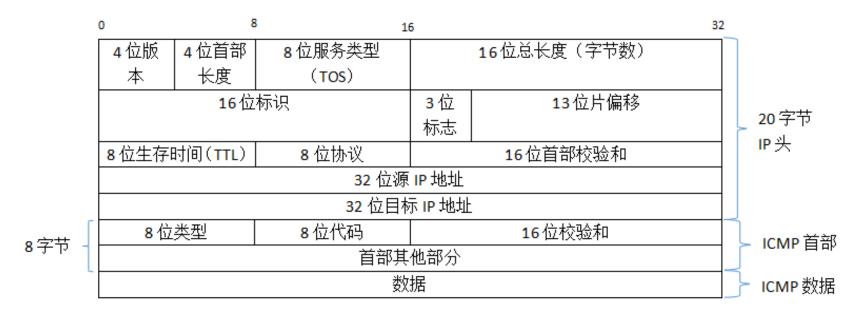
ICMP

- ICMP 是 "Internet Control Message Protocol" (网络控制报文协议)的缩写。
- 它是 TCP/IP 协议族的一个子协议,用于在 IP 主机、路由器之间传递控制消息。 控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。 这些控制消息虽然并不传输用户数据,但是对于用户数据的传递起着重要的作 用。
- ICMP 层区分不是很明显,一般划分在网络层中 通过 IP 包来封装ICMP数据,在实际传输中数据包的格式一般都是 IP 包 + ICMP包的格式,

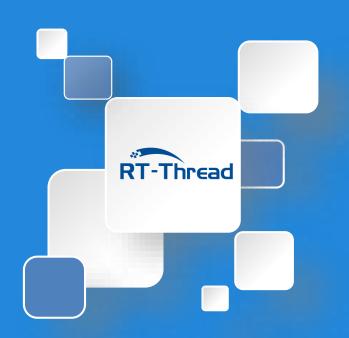


ICMP

- 具体格式如下:
 - IP 首部(20字节) + 8 位类型 + 8 位代码 + 16 位校验和 + ICMP 首部其他部分(7个字节) + 数据。
- 如果用图表的形式展现出来就是下面的这张图了







Ping 包分析

Ping 包分析

- 因为默认 ping 四次,所以加上两个 DNS 的数据包,最少可以抓到 10 个包,我们只看前四个就够了。第一个是域名解析的 DNS 请求包,第二个是 DNS 服务器回复的响应数据包,第三条是开发板发送给百度主机的请求包 (request)。第四条数据包是百度主机发送给开发板的一个回应(reply)的包。
- 我们也可以点开封包详细信息然后和 ICMP 协议的报文格式做对比,对 ping 的机制的理解会更加充分。

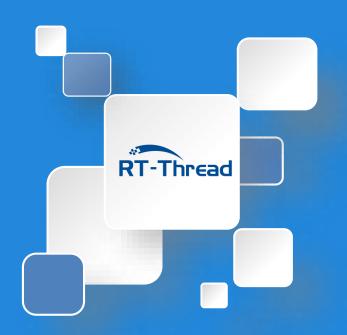


```
Internet Protocol Version 4, Src: 192.168.137.1, Dst: 192.168.137.135
    0100 .... = Version: 4
                                                                  前20个字节
    .... 0101 = Header Length: 20 bytes (5)
                                                                  是IP包,包
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
                                                                  含目标的 ip
    Identification: 0x0b5e (2910)
                                                                  和本机的 ip
  > Flags: 0x0000
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xdb89 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.137.1
    Destination: 192.168.137.135

▼ Internet Control Message Protocol

   Type: 8 (Echo (ping) request)
                               类型 8 为 ping的请求包
    Code: 0
    Checksum: 0x4d4d [correct]
                                                                    前8个字节
    [Checksum Status: Good]
                                                                   是协议头
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 14 (0x000e)
    Sequence number (LE): 3584 (0x0e00)
    [Response frame: 76]
    <del>Dala (32 byles)</del>
      Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
                                                                  最后是数据
      [Length: 32]
     RT··"3·· ·b·z··E·
                                                   -<-^--@- -----
0010 00 3c 0b 5e 00 00 40 01 db 89 c0 a8 89 01 c0 a8
                                                   ····MM·····abcdef这里是实际数据
0020 89 87 08 00 4d 4d 00 01 00 0e 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
                                                   ghijklmn opqrstuv
                                                                   上面是解析之后
0040 77 61 62 63 64 65 66 67 68 69
                                                   wabcdefg hi
                                                                   的数据
```





Ping 的过程

Ping 的过程

- 我们发起一个了从开发板到百度 www.baidu.com 的 ping 请求。(这里路由1 作为局域网的默认网关)
 - 首先开发板要解析百度的域名,获取到百度主机的 IP 地址,涉及到 DNS 协议,传输层用的是 UDP 协议。
 - DNS 主机利用 UDP 协议,回复百度的 IP 给开发板(这里也涉及了 ARP 协议暂时不讲)
 - 现在开发板要发送 Ping 请求包给百度主机,但是发现百度主机 IP 与自己不在同一网段, 因此要发送 Ping 请求包给<u>默认网关</u>。
 - 要发送给默认网关的时候,如果发现并没有默认网关对应的 MAC 地址,因此发送一个 ARP 广播包,如果交换机存储了默认网关的 MAC 地址,就直接告诉开发板默认网关的 MAC 地址,否则向所有端口发送 ARP 广播。

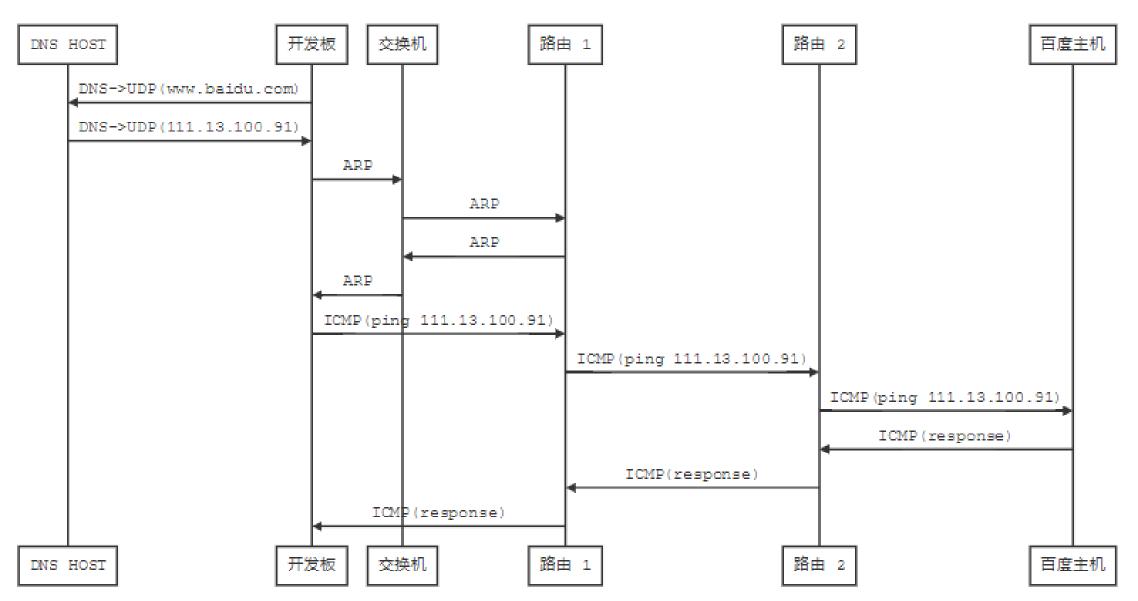


Ping 的过程

- 路由1收到了ARP请求报文后,单播自己的 MAC 地址给开发板。
- 这样开发板就可以把 Ping 包发送给默认网关(路由1)了。
- 然后路由1 通过<u>路由协议</u>,经过一个个路由的转发,最后发送到了百度的主机上。百度主机检测到 IP 是自己的 IP,接收并处理 Ping 请求,接着百度主机发送一个 Ping 回应报文给开发板。



Dia 443十千日



RT-Thread