

# 以太网帧分析实验

学生姓名：李俊杰 1850668

合作学生：无

实验地点：济事楼 330

实验时间：2020 年 11 月 27 日 78 节

## 【实验目的】

- 1.通过实验熟悉以太网物理帧数据结构。
- 2.通过实验进一步了解 IP 数据包封装机制。
- 3.通过实验体会网络体系分层结构设计原理及其优势。
- 4.掌握抓取、分析各种数据包的操作。

## 【实验原理】

### 1.以太网简介

以太网是一种计算机局域网技术（LAN），是目前应用最普遍的局域网技术。IEEE 组织制定了以太网的技术标准，称为 IEEE 802.3，它规定了包括物理层的连线、电子信号和介质访问层协议的内容。

### 2.以太网分类

以太网是现实世界中最普遍的一种计算机网络，分为两类：第一类称为经典以太网，第二类称为交换式以太网，使用了一种称为交换机的设备连接不同的物理设备。

经典以太网是以太网的原始形式，运行速度在 3-10Mbps，而交换式以太网是应用最广泛的以太网，可运行在 100、1000 和 10000Mbps 的高速率链路上，相应速率的以太网称为以太网、千兆以太网和万兆以太网。

### 3.以太网拓扑结构

以太网的标准拓扑结构为总线型拓扑。但目前的快速以太网（100BASE-T、1000BASE-T 标准）为了减少冲突，使用交换机来进行网络组织和连接，大大提高了网络速度并使效率最大化，因此相应的以太网拓扑结构转变为星型，

但在逻辑上以太网仍然使用总线型拓扑和带有冲突检测的载波监听多路访问（CSMA/CD, Carrier Sense Multiple Access with Collision Detection）技术。

#### 4.以太网地址（MAC）

每一个节点都有一个全球唯一的 48 位地址，即制造商分配给网卡的 MAC 地址，以保证以太网上所有节点能够互相鉴别，由于以太网的广泛应用，许多制造商已经将以太网卡直接集成进计算机主板。

MAC 地址又称为物理地址、硬件地址，由网络设备制造商生产时烧录在网卡（Network Interface Card, NIC 网络接口卡）的 EPROM 中。MAC 地址长度为 48 位（6 个字节），通常表示为 12 个 16 进制数，如 MAC 地址 00-16-EA-AE-3C-40，其中前 3 个字节由 IEEE 分配给网络设备制造商，代表网络设备硬件制造商，用以区分不同的生产厂家，即 OUI（Organizationally Unique Identifier），而后 3 个字节由网络设备制造商分配，代表某个网络产品（如网卡）的系列号，MAC 地址在全世界是唯一的。

其中 MAC 地址最高字节（MSB）的低第二位（LSB）表示这个 MAC 地址是全局的还是本地的，即 U/L（Universal / Local）位，如果为 0 表示全局地址，如果为 1 表示本地地址，所有的 OUI 这一位都是 0。MAC 地址最高字节（MSB）的低第一位（LSB）表示这个 MAC 地址是单播还是组播的，0 表示单播。

#### 5.MAC 数据包格式

前导码和帧开始符：一个帧以 7 个字节的前导码和 1 个字节的帧作为帧的开始，其相应的 16 进制表示为 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0xD5。

报头：报头包含源地址和目标地址的 MAC 地址，以太网类型字段和可选的用于说明 VLAN 成员关系和传输优先级的 IEEE 802.1Q VLAN 标签。

帧校验码：帧校验码是一个 32 位循环冗余校验码（CRC），以便验证帧数据是否被损坏。

帧间距：当一个帧发送出去之后，发送方在下次发送帧之前，需要发送至少 12 个 octet 的空闲线路状态码。

以太网帧类型：以太网还有很多种类型，不同类型的帧具有不同的格式和 MTU 值，但在不同物理媒体上都可以同时存在。以太网第二版的帧称之为 Ethernet II 帧，DIX 帧，是最常见的帧类型，通常直接被 IP 协议使用。

6.Ethernet II



图 4-14 帧格式  
(a) 以太网 (DIX)；(b) IEEE 802.3

802.3 以太网帧结构								
前导码	帧开始符	MAC 目标地址	MAC 源地址	802.1Q 标签 (可选)	以太类型	负载	冗余校验	帧间距
10101010 7个octet	10101011 1个octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
64-1522 octets								
72-1530 octets								
84-1542 octets								

以太 II 帧（也称作 DIX 以太网），是以这个设计的主要成员 DEC、Intel 和 Xerox 名字命名的，其把紧接在目标和源 MAC 地址后面的这两个字节定义为以太网帧数据类型字段。例如，一个 0x0800 的以太网类型说明这个帧包含的是 IPv4 类型数据包，同样的一个 0x0806 的以太网类型说明这个帧是一个 ARP 帧，0x8100 说明这是一个 IEEE802.1Q 帧，而 0x86DD 说明这个是一个 IPv6 帧。

当这个工业界的标准通过正式的 IEEE 标准化进程后，在 802.3 标准中以太网类型字段变成了一个数据长度字段，最初的以太网通过包含它们的帧来确定它们的长度，而不是以一个明确的数值。但是包的接受层仍然需要知道如何解析包，因此标准规定将 IEEE802.2 头跟在长度字段后面定义包的类型，在很多年之后的 802.3x-1997 标准中（一个 802.3 标准的后继版本）正式允许两种数据类型的数据包同时存在。

实际上两种数据包都被广泛使用，而最初的以太网数据包在以太网局域网中广泛应用，因为其简便和低开销。为了允许一些使用以太 II 帧的数据包和一些使用 802.3 封装的最初低版本数据包能够在一个网段使用，以太网类型值必

须大于等于 1536（0x0600），这个值比 802.3 数据包的最大长度 1500byte（0x05DC）要更大。这样如果这个字段的值大于等于 1536，则这个帧是以太 II 帧，相应的字段为类型字段，否则（小于 1500 而大于 46 字节）就是一个 802.3 帧，相应字段为长度字段，1500-1536 的数值未定义。

### 【实验设备】

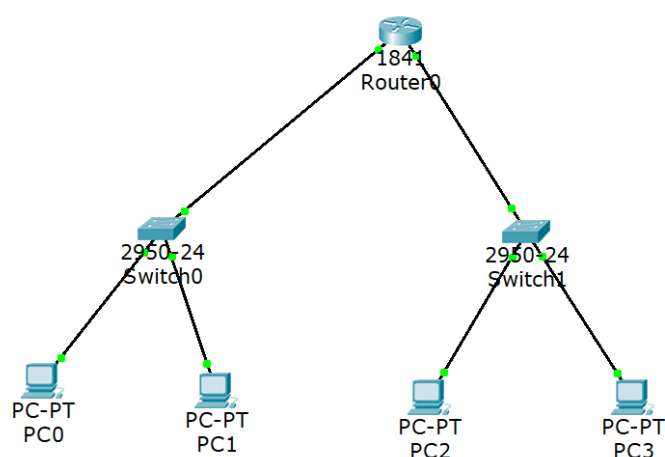
- 1.一台运行 Windows 系统的计算机。
- 2.网络终端模拟仿真软件 Cisco Packet Tracer。
- 3.网络抓包软件 WireShark。

### 【实验步骤】

- 1.首先规划网络地址及其拓扑结构。
- 2.路由器接口 IP 地址配置。
- 3.配置 DHCP 之前检查 PC 是否存在 IP 地址。
- 4.在 R0 上配置 DHCP。
- 5.验证各个 PC 的 IP 地址。

### 【实验现象】

- 1.首先规划网络地址及其拓扑结构。



- 2.路由器相关接口配置：

相关操作命令如下：

```
interface FastEthernet 0/0
```

```
ip address 192.168.1.1 255.255.255.0
```

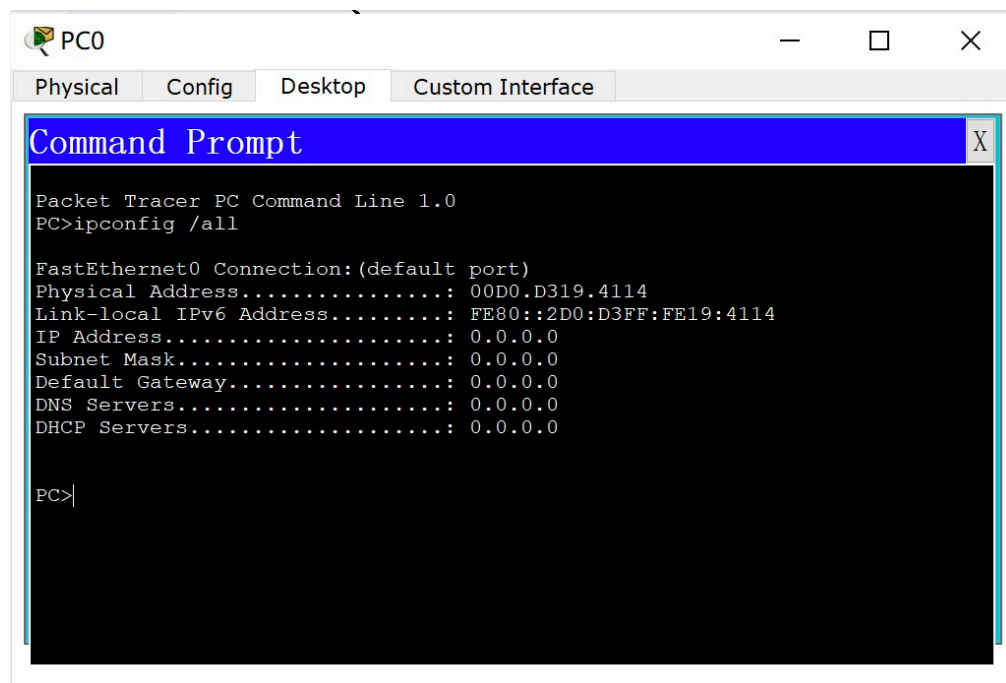
```
no shutdown
```

```
interface FastEthernet 0/1
```

```
ip address 192.168.2.1 255.255.255.0
```

```
no shutdown
```

3.配置 DHCP 之前检查相关 PC 的 IP 地址。



3.配置 R0 路由器 DHCP。

路由器左边网络 DHPC 配置：

```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
```

```
ip dhcp pool myleftnet
```

```
network 192.168.1.0 255.255.255.0
```

```
default-router 192.168.1.1
```

```
option 150 ip 192.168.1.3
```

```
dns-server 192.168.1.2
```

路由器右边网络 DHCP 配置：

ip dhcp excluded-address 192.168.2.0 192.168.2.10

ip dhcp pool myrightnet

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

option 150 ip 192.168.2.3

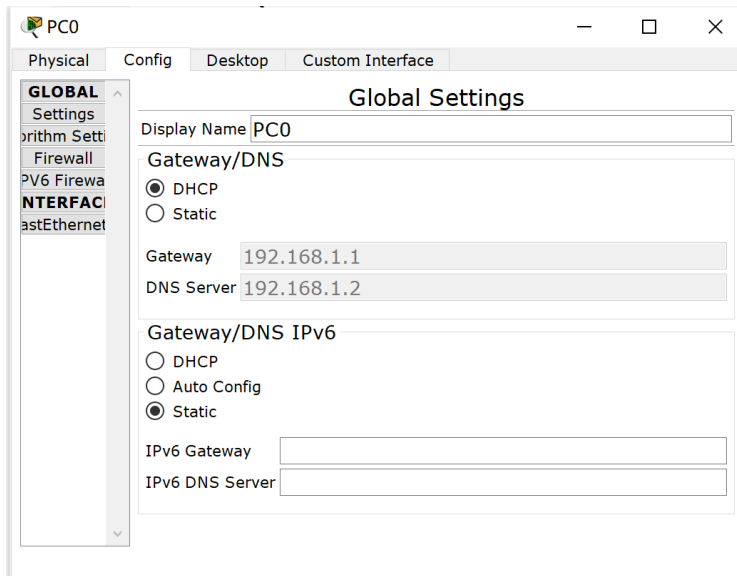
dns-server 192.168.2.2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown

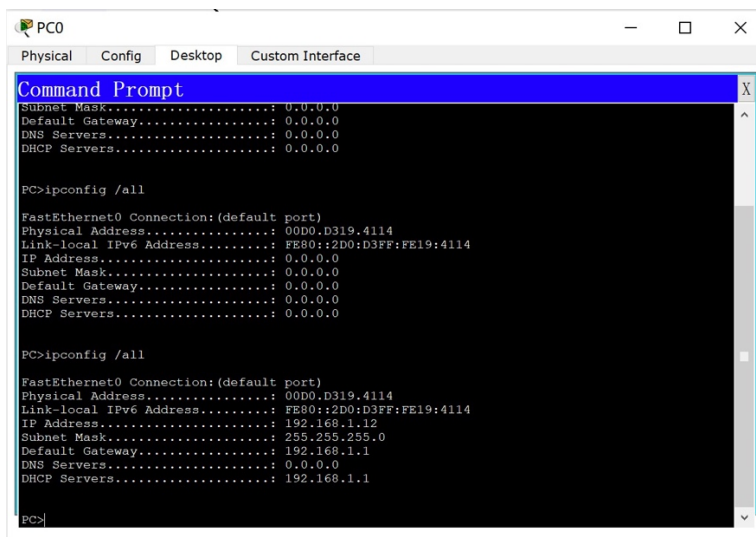
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
ip address 192.168.1.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
ip address 192.168.2.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#exit
Router(config)#ip dhcp
Router(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.10
Router(config)#ip dhcp pool leftnet
Router(config)#ip dhcp pool leftnet net
Router(config)#ip dhcp pool leftnet
Router(config)#ip dhcp pool leftnet
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#option 150 ip 192.168.1.3
Router(dhcp-config)#dns-server 192.168.1.2
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.2.0 192.168.2.10
Router(config)#ip dhcp pool rightnet
Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#option 150 ip 192.168.2.3
Router(dhcp-config)#dns-server 192.168.2.2
Router(dhcp-config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

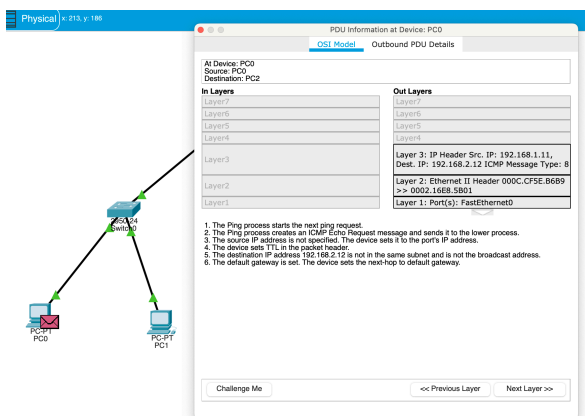
并打开各台 PC DHCP 获取 IP 地址服务。



4.配置 DHCP 后查看各台 PC 的 IP 地址。



5.查看数据包，模拟 ICMP 从 PC0 到 PC2 数据包，并查看相关数据。



PDU Information at Device: Switch0

**OSI Model**   Inbound PDU Details   Outbound PDU Details

At Device: Switch0  
Source: PC0  
Destination: PC2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer 2: Ethernet II Header 000C.CF5E.B6B9 >> 0002.16E8.5B01	Layer 2: Ethernet II Header 000C.CF5E.B6B9 >> 0002.16E8.5B01
Layer 1: Port FastEthernet0/2	Layer 1: Port(s): FastEthernet0/1

1. FastEthernet0/2 receives the frame.

Challenge Me   << Previous Layer   Next Layer >>

PDU Information at Device: Router0

**OSI Model**   Inbound PDU Details   Outbound PDU Details

At Device: Router0  
Source: PC0  
Destination: PC2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.12 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 192.168.1.11, Dest. IP: 192.168.2.12 ICMP Message Type: 8
Layer 2: Ethernet II Header 000C.CF5E.B6B9 >> 0002.16E8.5B01	Layer 2:
Layer 1: Port FastEthernet0/0	Layer1

1. FastEthernet0/0 receives the frame.

Challenge Me   << Previous Layer   Next Layer >>

PDU Information at Device: Router0

**OSI Model**   Outbound PDU Details

At Device: Router0  
Source: Router0  
Destination: Broadcast

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer3
Layer2	Layer 2: Ethernet II Header 0002.16E8.5B02 >> FFFF.FFFF.FFFF ARP Packet Src. IP: 192.168.2.1, Dest. IP: 192.168.2.12
Layer1	Layer 1: Port(s): FastEthernet0/1

1. The ARP process constructs a request for the target IP address.  
2. The device encapsulates the PDU into an Ethernet frame.

Challenge Me   << Previous Layer   Next Layer >>



### PDU Information at Device: Switch1

OSI Model
Inbound PDU Details
Outbound PDU Details

At Device: Switch1  
 Source: Router0  
 Destination: Broadcast

**In Layers**  
 Layer7  
 Layer6  
 Layer5  
 Layer4  
 Layer3  

Layer 2: Ethernet II Header  
 0002.16E8.5B02 >>  
 FFFF.FFFF.FFFF ARP Packet Src. IP:  
 192.168.2.1, Dest. IP:  
 192.168.2.12

Layer 1: Port FastEthernet0/1

**Out Layers**  
 Layer7  
 Layer6  
 Layer5  
 Layer4  
 Layer3  

Layer 2: Ethernet II Header  
 0002.16E8.5B02 >>  
 FFFF.FFFF.FFFF ARP Packet Src. IP:  
 192.168.2.1, Dest. IP:  
 192.168.2.12

Layer 1: Port(s): FastEthernet0/2  
 FastEthernet0/3

1. FastEthernet0/1 receives the frame.

Challenge Me
<< Previous Layer
Next Layer >>

### PDU Information at Device: PC2

OSI Model
Inbound PDU Details
Outbound PDU Details

At Device: PC2  
 Source: Router0  
 Destination: Broadcast

**In Layers**  
 Layer7  
 Layer6  
 Layer5  
 Layer4  
 Layer3  

Layer 2: Ethernet II Header  
 0002.16E8.5B02 >>  
 FFFF.FFFF.FFFF ARP Packet Src. IP:  
 192.168.2.1, Dest. IP:  
 192.168.2.12

Layer 1: Port FastEthernet0


**Out Layers**  
 Layer7  
 Layer6  
 Layer5  
 Layer4  
 Layer3  

Layer 2: Ethernet II Header  
 0030.F2CB.136A >>  
 0002.16E8.5B02 ARP Packet Src.  
 IP: 192.168.2.12, Dest. IP:  
 192.168.2.1

Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.

Challenge Me
<< Previous Layer
Next Layer >>

Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	Router0	ICMP
	0.003	Router0	Switch1	ICMP
	0.004	Switch1	PC2	ICMP
	0.005	PC2	Switch1	ICMP
	0.006	Switch1	Router0	ICMP
	0.007	Router0	Switch0	ICMP
	0.008	Switch0	PC0	ICMP
	0.707	--	Switch0	STP

6.练习使用 Wireshark 软件，查看 DIX V2 帧。

No.	Time	Source	Destination	Protocol	Length	Info
6	1.742795	100.68.227.99	157.240.9.18	TCP	78	54012 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=604861653 TSecr=0 SACK_PERM=1
7	1.866807	109.244.152.17	100.68.227.99	TCP	238	8080 → 53491 [PSH, ACK] Seq=369 Ack=1 Win=63 Len=184
8	1.866337	100.68.227.99	109.244.152.17	TCP	54	53491 → 8080 [ACK] Seq=1 Ack=553 Win=4096 Len=0
9	4.607559	109.244.152.17	100.68.227.99	TCP	238	8080 → 53491 [PSH, ACK] Seq=553 Ack=1 Win=63 Len=184
10	4.607971	100.68.227.99	109.244.152.17	TCP	54	53491 → 8080 [ACK] Seq=1 Ack=737 Win=4096 Len=0
11	6.955691	100.68.227.99	60.191.83.6	TCP	66	52716 → 443 [FIN, ACK] Seq=1 Ack=1 Win=2859 Len=0 TSval=604866661 TSecr=1282284113
12	6.974784	100.68.227.99	60.191.83.6	TCP	78	54029 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=604866880 TSecr=0 SACK_PERM=1
13	6.988079	60.191.83.6	100.68.227.99	TCP	74	443 → 54029 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1386 SACK_PERM=1 TSval=1283183712 TSecr=6048668
14	6.988214	100.68.227.99	60.191.83.6	TCP	66	54029 → 443 [ACK] Seq=1 Ack=1 Win=13184 Len=0 TSval=604866893 TSecr=1283183712
15	6.998194	100.68.227.99	60.191.83.6	TCP	248	54029 → 443 [PSH, ACK] Seq=1 Ack=1 Win=13184 Len=182 TSval=604866902 TSecr=1283183712 [TCP segment of
16	7.010962	60.191.83.6	100.68.227.99	TCP	66	443 → 54029 [ACK] Seq=1 Ack=183 Win=15616 Len=0 TSval=1283183736 TSecr=604866902
17	7.014165	60.191.83.6	100.68.227.99	SSL	77	Continuation Data
18	7.014282	100.68.227.99	60.191.83.6	TCP	66	54029 → 443 [ACK] Seq=183 Ack=12 Win=13184 Len=0 TSval=604866917 TSecr=1283183737
19	7.014572	100.68.227.99	60.191.83.6	TCP	238	54029 → 443 [PSH, ACK] Seq=183 Ack=12 Win=13184 Len=172 TSval=604866917 TSecr=1283183737 [TCP segment.
20	7.068059	60.191.83.6	100.68.227.99	TCP	66	443 → 54029 [ACK] Seq=12 Ack=355 Win=16640 Len=0 TSval=1283183792 TSecr=604866917
21	7.068174	100.68.227.99	60.191.83.6	TCP	702	54029 → 443 [PSH, ACK] Seq=355 Ack=12 Win=13184 Len=636 TSval=604866970 TSecr=1283183792 [TCP segment.
22	7.080787	60.191.83.6	100.68.227.99	TCP	66	443 → 54029 [ACK] Seq=12 Ack=991 Win=17920 Len=0 TSval=1283183806 TSecr=604866970
> Frame 16: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0 > Ethernet II, Src: New3Cte_55:92:01 (48:bd:3d:55:92:01), Dst: Apple_33:fc:b4 (f0:18:98:33:fc:b4) > Destination: Apple_33:fc:b4 (f0:18:98:33:fc:b4) Address: Apple_33:fc:b4 (f0:18:98:33:fc:b4) ....0. .... = LG bit: Globally unique address (factory default) ....0. .... = IG bit: Individual address (unicast) > Source: New3Cte_55:92:01 (48:bd:3d:55:92:01) Address: New3Cte_55:92:01 (48:bd:3d:55:92:01) ....0. .... = LG bit: Globally unique address (factory default) ....0. .... = IG bit: Individual address (unicast) Type: IPv4 (8x8080) > Internet Protocol Version 4, Src: 60.191.83.6, Dst: 100.68.227.99 > Transmission Control Protocol, Src Port: 443, Dst Port: 54029, Seq: 1, Ack: 183, Len: 0						
0000	f0 18 98 33 fc b4 48 bd	3d 55 92 01 08 00 45 00	---3---H: =U---E:			
0010	00 34 e0 83 40 00 31 06	91 d3 3c bf 53 06 64 44	4 @ 1 < S dD			
0020	e3 03 01 30 d3 05 11 d0	24 ee b4 8f d4 6e 08 10	c .... 4 . n			
0030	00 7a 2b fc 00 00 01 01	08 0a 4c 7b d4 78 24 0d	z+-----L( x\$			
0040	89 56		V			

## 【分析讨论】