



计算机网络实验二

以太网协议 (Ethernet)

信息学部 朱婉婷

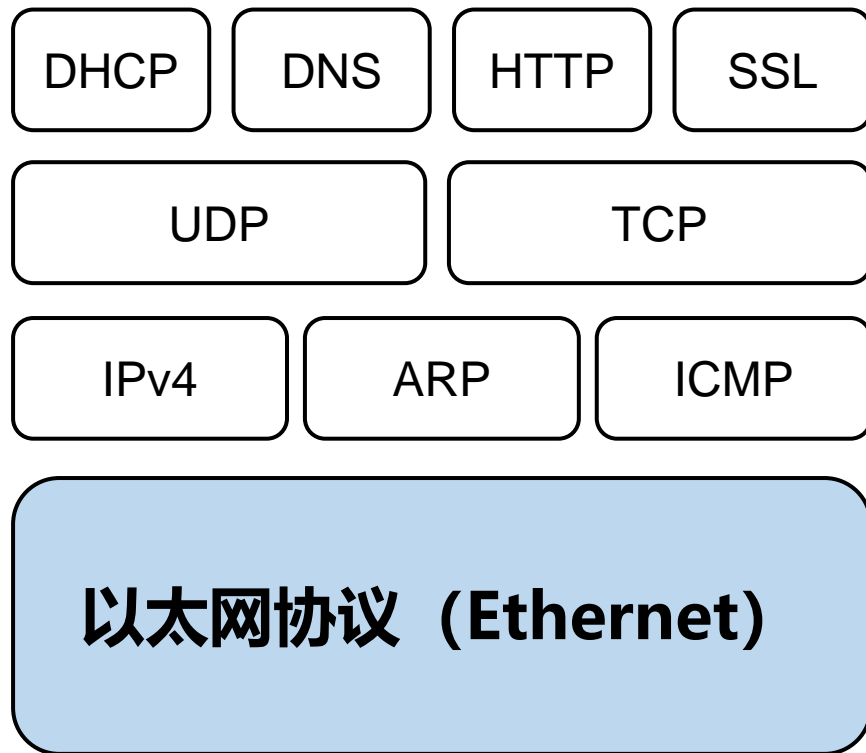
主要内容

- 一、实验原理
- 二、单播帧抓包实验
- 三、广播帧抓包实验
- 四、多播帧抓包实验

以太网协议 (Ethernet) 介绍

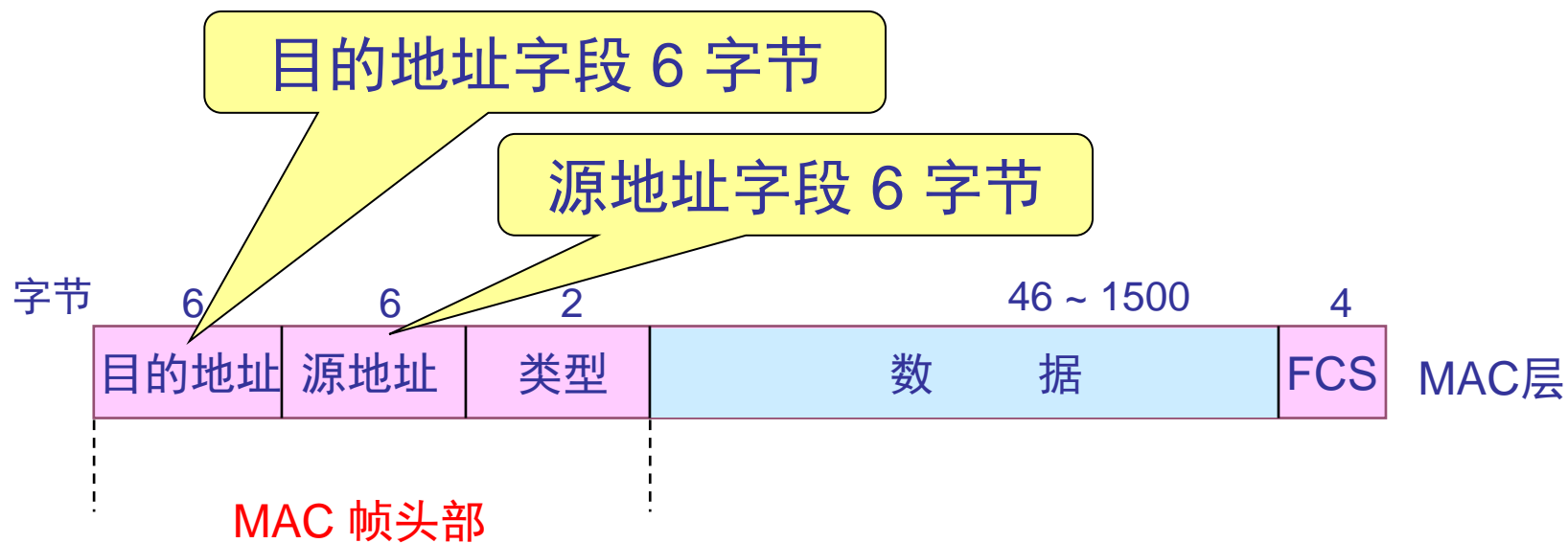
◆以太网的两个标准

- DIX的 **Ethernet II** 是世界上第一个局域网产品（以太网）的规约。
- **IEEE 802.3** 标准。
- “以太网”一般是指符合Ethernet II标准的局域网。



以太网帧格式

◆Ethernet II标准的MAC帧格式



以太网帧格式

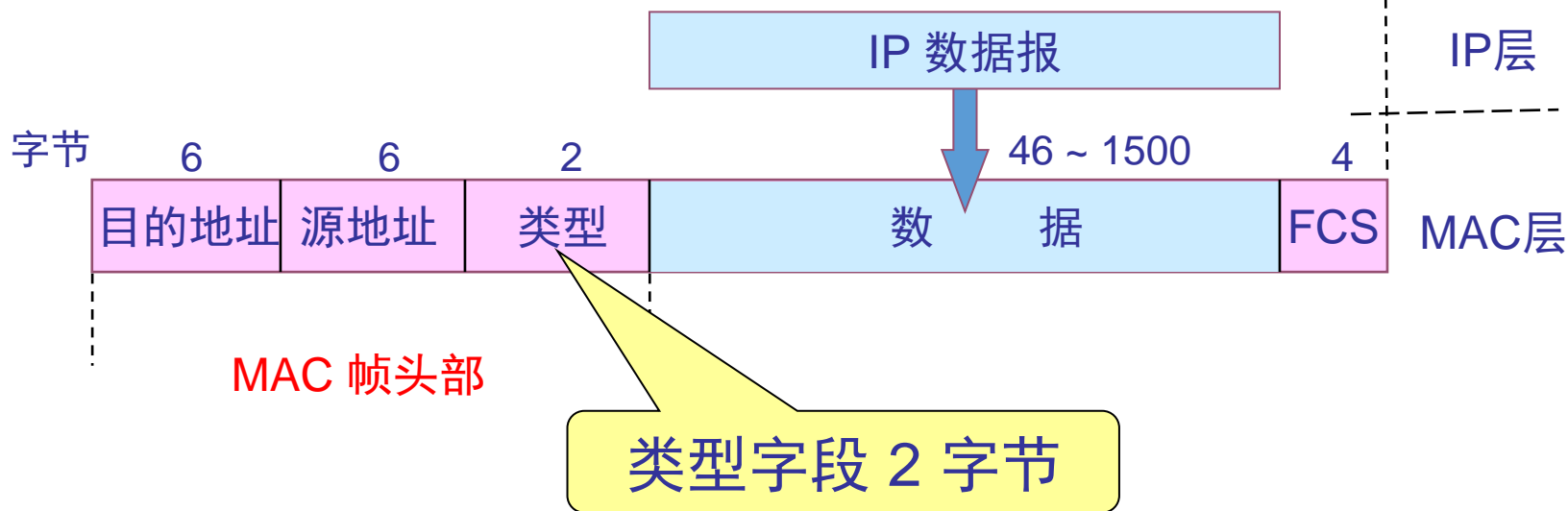
◆目的地址、源地址（各6字节）

- 48 位的 MAC 地址。
- 在局域网中，硬件地址又称为物理地址，或 MAC 地址。
- 实际上就是网卡地址，它的通用名称是EUI-48。
- IEEE 的注册管理机构 RA 负责向厂家分配地址字段的前三个字节(即高位 24 位)。
- 地址字段中的后三个字节(即低位 24 位)由厂家自行指派，称为扩展标识符，必须保证生产出的网卡没有重复地址。

以太网帧格式

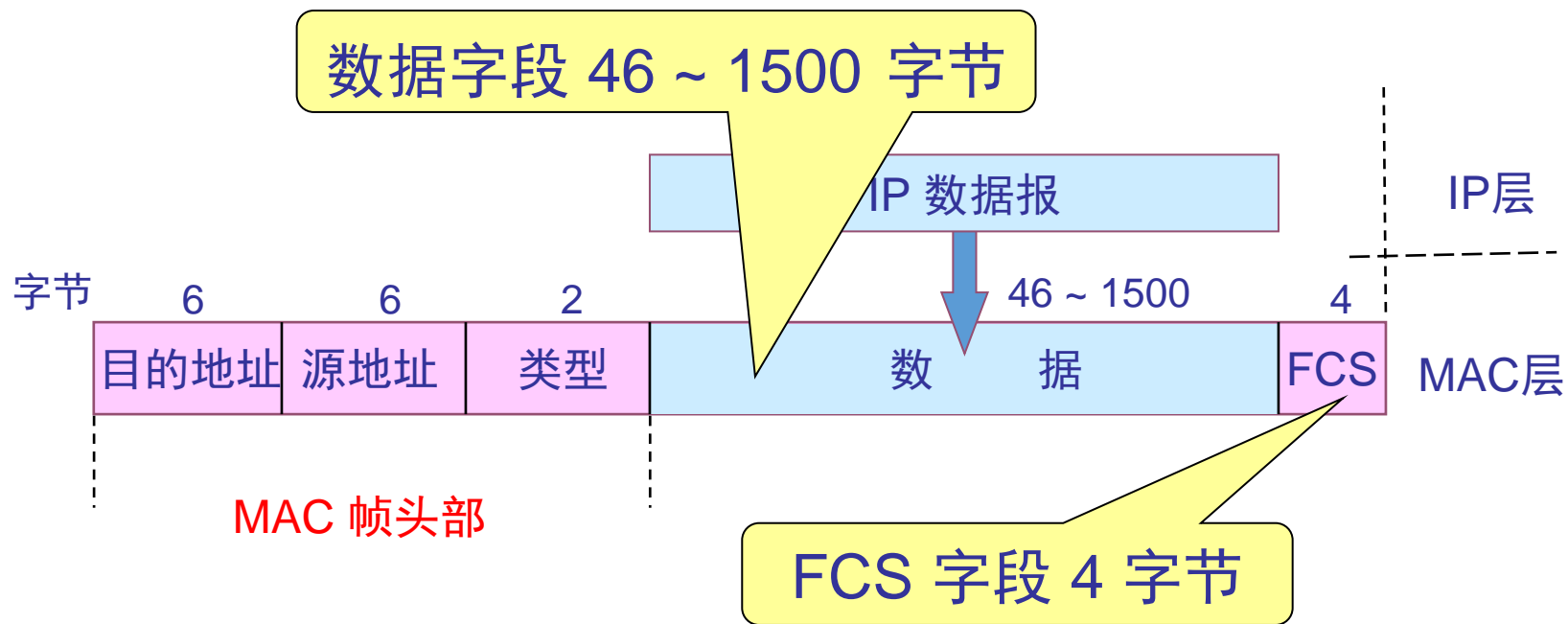
◆类型 (2字节)

- 类型字段用来标志~~上~~一层使用的是什么协议，以便把收到的 MAC 帧的数据上交给上层的这个协议。



以太网帧格式

◆Ethernet II标准的MAC帧格式



以太网帧格式

◆数据字段 (46 ~ 1500 字节)

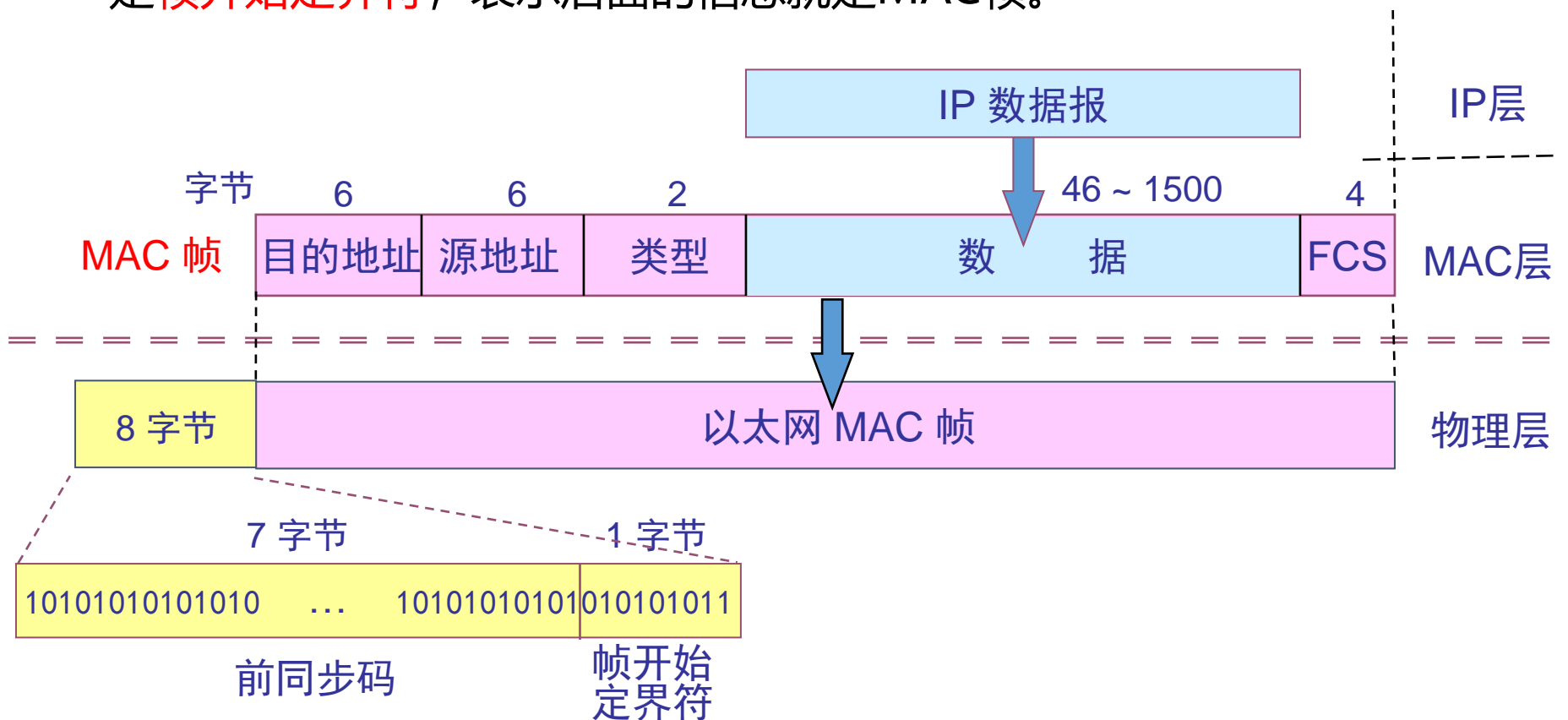
- 数据字段的最小长度46字节 =
MAC帧最小长度 64 字节 - 18 字节的首部和尾部
- 当数据字段的长度小于46字节时，应在数据字段的后面加入整数字节的填充字段。以保证以太网的MAC 帧长不小于64字节。

◆FCS 字段 (4 字节)

- 在数据后面添加上的冗余码称为帧检验序列FCS (Frame Check Sequence)。
- 链路层常用的检错方法是循环冗余校验码CRC。

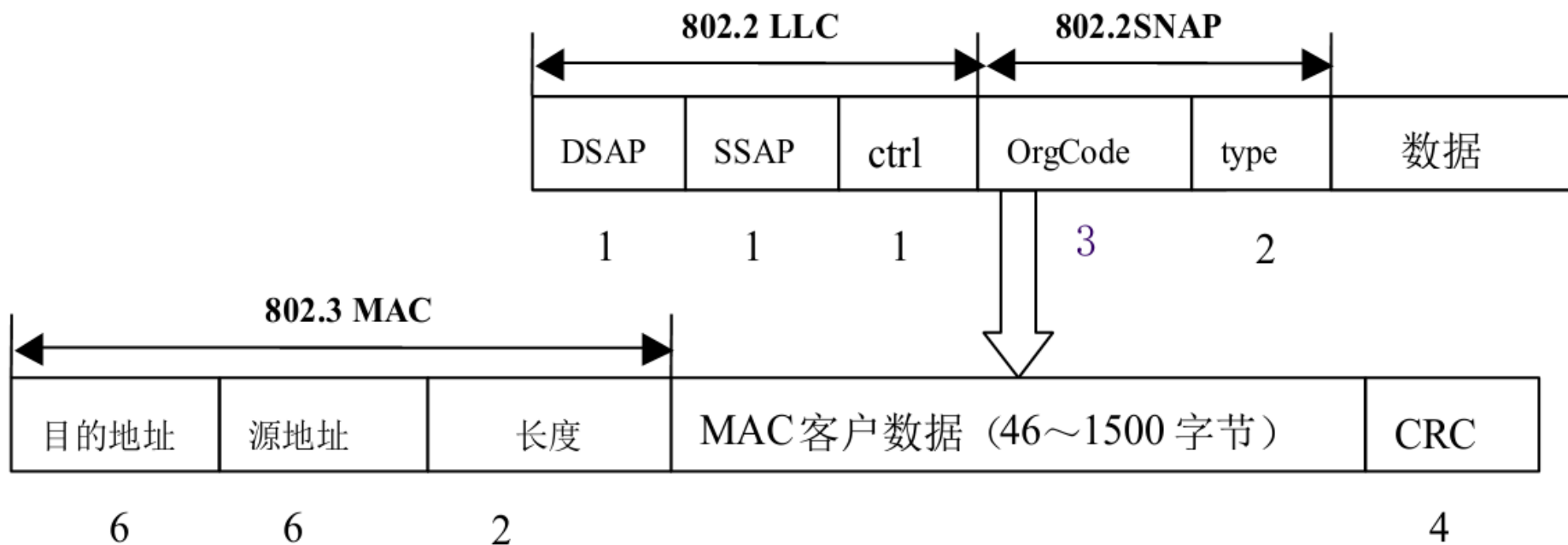
以太网帧格式

注：实际上，在传输媒介上传送的要比MAC帧还多8个字节。其中7个字节是**前同步码**，用来迅速实现MAC帧的比特同步；1个字节是**帧开始定界符**，表示后面的信息就是MAC帧。



以太网帧格式

◆ IEEE 802.3标准的MAC帧格式



IEEE 802.3报文封装结构

主要内容

- 一、实验原理
- 二、单播帧抓包实验
- 三、广播帧抓包实验
- 四、多播帧抓包实验

实验环境搭建

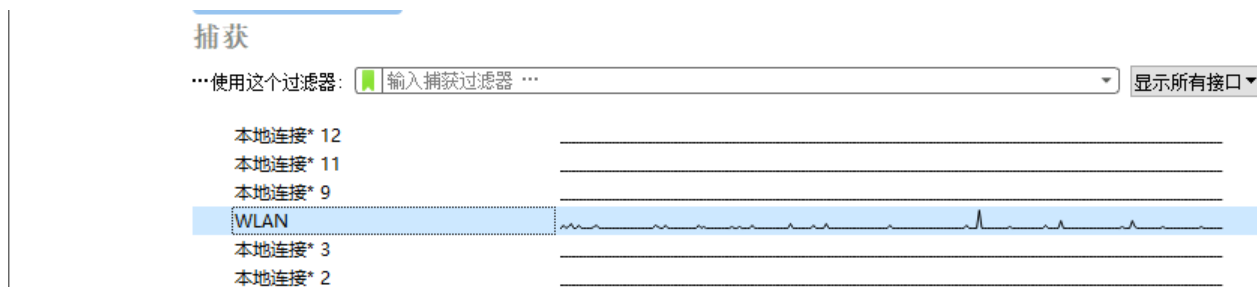
列出本次实验所使用的平台和相关软件，以下为例：

(打开cmd指令窗口，输入指令 “ipconfig /all”查看)

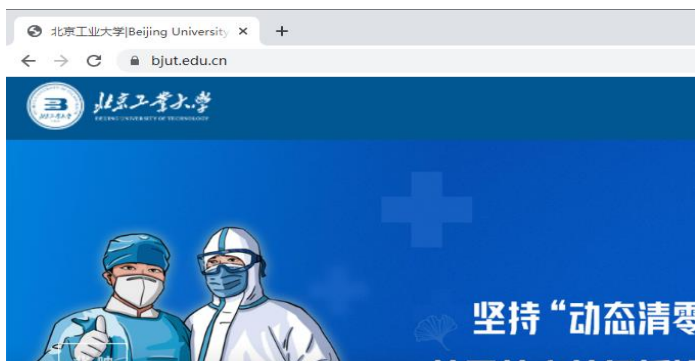
- 1、主机：联想笔记本（Win10系统）；主机IP地址：192.168.1.106；子网掩码：255.255.255.0；主机网卡MAC地址：34-F6-4B-C0-90-40。
- 2、网络连接方式：无线连接；默认网关地址：192.168.1.1。
- 3、抓包工具：Wireshark（v3.6.2）。

实验具体步骤

1、打开Wireshark软件，双击本次实验正在使用的网络接口，开始进行抓包。



2、然后打开浏览器，在网页地址栏中输入网址，例如对北京工业大学官网进行访问，浏览校园新闻。



The image shows the Wireshark packet capture window. The top menu bar includes '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)', and '帮助(H)'. Below the menu bar is a toolbar with various icons. The main area displays a list of captured packets with columns for 'No.', 'Time', 'Source', 'Destination', 'Protocol', 'Length', and 'Info'. The packets are listed in a table format.

No.	Time	Source	Destination	Protocol	Length	Info
16	3.644233	192.168.1.106	224.0.0.252	IGMPv2	46	Membr
17	3.644280	fe80::ed46:e42f:c3f...	ff02::16	ICMPv6	150	Mult
18	4.326913	192.168.1.106	142.251.42.234	TCP	66	6058
19	4.605835	192.168.1.106	142.251.42.234	TCP	66	[TCP
20	6.613433	192.168.1.106	142.251.42.234	TCP	66	[TCP
21	7.744674	Tp-LinkT_57:29:ad	IntelCor_c0:90:40	ARP	42	Who
22	7.744695	IntelCor_c0:90:40	Tp-LinkT_57:29:ad	ARP	42	192.
23	8.633956	192.168.1.106	221.181.99.20	TCP	488	5808
24	8.665039	221.181.99.20	192.168.1.106	TCP	54	80 →
25	8.719730	221.181.99.20	192.168.1.106	TCP	144	80 →
26	8.764918	192.168.1.106	221.181.99.20	TCP	54	5808
27	10.523536	120.133.59.141	192.168.1.106	TLSv1.2	85	Encr
28	10.523536	120.133.59.141	192.168.1.106	TCP	54	443

单播帧抓包实验实例

3、使用本机IP地址和协议名对捕获的数据包进行筛选。

过滤表达式如下: `ip.addr == 192.168.1.106 and eth`

4、从中选取任一单播数据包, 观察MAC帧格式, 并进行分析。

The image shows a Wireshark packet capture interface. A red arrow points to the filter bar at the top, which contains the expression `ip.addr == 192.168.1.106 and eth`. Below the filter bar is a list of captured packets. Packet 13 is highlighted with a red box. The detailed view of packet 13 is shown below the list, with a red box highlighting the Ethernet II section, specifically the destination MAC address: `Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)`. A red arrow points to this MAC address.

No.	Time	Source	Destination	Protocol	Length	Info
12	2.809134	192.168.1.106	112.13.121.32	TLSv1.2	92	Application Data
13	2.843473	112.13.121.32	192.168.1.106	TCP	54	443 → 58203 [ACK] Seq=35 Ack=39 Win=0 Len=0
14	2.895389	192.168.1.106	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
15	4.514774	192.168.1.106	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
16	5.014554	192.168.1.106	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
17	5.373031	120.133.59.141	192.168.1.106	TLSv1.2	85	Encrypted Alert
18	5.373031	120.133.59.141	192.168.1.106	TCP	54	443 → 58963 [FIN, ACK] Seq=32 Ack=1 Len=0

> Frame 13: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF {B601EEAA-316D-44F3-A63C-...}

> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)

> Internet Protocol Version 4, Src: 112.13.121.32, Dst: 192.168.1.106

> Transmission Control Protocol, Src Port: 443, Dst Port: 58203, Seq: 35, Ack: 39, Len: 0

实验结果与分析

实验结果:

No.	Time	Source	Destination	Protocol	Length	Info
13	2.843473	112.13.121.32	192.168.1.106	TCP	54	443 → 58203 [ACK] Seq=35 Ack=39
<						
> Frame 13: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B601EEAA-316D-4}						
▼ Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)						
▼ Destination: IntelCor_c0:90:40 (34:f6:4b:c0:90:40) ←						
Address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)						
....0. = LG bit: Globally unique address (factory default)						
....0. = IG bit: Individual address (unicast) ←						
▼ Source: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad) ←						
Address: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)						
....0. = LG bit: Globally unique address (factory default)						
....0. = IG bit: Individual address (unicast)						
Type: IPv4 (0x0800) ←						
<						
0000	34 f6 4b c0 90 40 f4 2a 7d 57 29 ad 08 00	45 d4	4·K··@·* }W)···E·			
0010	00 28 64 1e 40 00 33 06 37 9e 70 0d 79 20 c0 a8	·(d@·3· 7·p·y ··				
0020	01 6a 01 bb e3 5b 99 12 ac 1d c3 9f 2f 18 50 10	·j···[·· ····/·P·				
0030	00 06 e7 8f 00 00				

实验结果与分析

实验分析：

- 目的MAC地址： 34:f6:4b:c0:90:40
- 源MAC地址： f4:2a:7d:57:29:ad
- 类型： 0x0800，上层协议为IPv4协议
- 数据字段：可见字节长度为40字节，包含IPv4头部和TCP段。
- FCS：不可见

实验结果与分析

绘制以太网帧格式：

目的MAC地址	源MAC地址	帧内封装的上层协议类型	数据	FCS
34:f6:4b:c0:90:40	f4:2a:7d:57:29:ad	IPv4 (0x0800)	40字节（封装的上层协议包内容）	不可见

思考题

思考题：在计算机网络课程学习中，Ethernet II规定了以太网MAC层的报文格式分为7字节的前导符、1字节的起始符、6字节的目的MAC地址、6字节的源MAC地址、2字节的类型、数据字段和4字节的数据校验字段。对于选中的报文，缺少哪些字段，为什么？

主要内容

- 一、实验原理
- 二、单播帧抓包实验
- 三、广播帧抓包实验
- 四、多播帧抓包实验

广播帧抓包实验实例

5、使用广播地址对捕获的数据包进行筛选。

过滤表达式如下：eth.addr == ff:ff:ff:ff:ff:ff

6、从中选取任一广播数据包，观察MAC帧格式，并进行分析。

The image shows a Wireshark packet capture interface. A red arrow points to the filter bar at the top, which contains the expression `eth.addr == ff:ff:ff:ff:ff:ff`. Below the filter bar, a table of captured packets is displayed. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet list shows several packets, with packet 8 highlighted. A red box highlights the entire row for packet 8. Below the packet list, the details pane for packet 8 is expanded, showing the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data sections. A red box highlights the Ethernet II section, specifically the destination address field, which is `Broadcast (ff:ff:ff:ff:ff:ff)`. A red arrow points to this field.

No.	Time	Source	Destination	Protocol	Length	Info
7	0.921308	Tp-LinkT_57:29:ad	Broadcast	ARP	60	Who has 192.168.1.101? T
8	1.228782	192.168.1.1	255.255.255.255	UDP	174	59249 → 5001 Len=132
10	1.945541	Tp-LinkT_57:29:ad	Broadcast	ARP	60	Who has 192.168.1.101? T
108	21.503538	192.168.1.1	255.255.255.255	UDP	174	59249 → 5001 Len=132

> Frame 8: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{B601...}

> Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255

> User Datagram Protocol, Src Port: 59249, Dst Port: 5001

> Data (132 bytes)

实验结果与分析

实验结果:

No.	Time	Source	Destination	Protocol	Length	Info
8	1.228782	192.168.1.1	255.255.255.255	UDP	174	59249 → 5001 Len=132
<						
> Frame 8: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{B601EEAA-316}						
▼ Ethernet II, Src: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad), 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: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)						
Address: Tp-LinkT_57:29:ad (f4:2a:7d:57:29:ad)						
.... 0. = LG bit: Globally unique address (factory default)						
.... 0 = IG bit: Individual address (unicast)						
Type: IPv4 (0x0800)						
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 255.255.255.255						
> User Datagram Protocol, Src Port: 59249, Dst Port: 5001						
> Data (132 bytes)						
<						
0000	ff ff ff ff ff f4 2a 7d 57 29 ad 08 00	45 00* }W)...	E.		
0010	00 a0 00 00 40 00 40 11 78 a4 c0 a8 01 01 ff ff		...@.@. x.....			
0020	ff ff e7 71 13 89 00 8c 42 32 01 01 0e 00 e1 2b		...q.... B2.....+			
0030	83 c7 dc 90 00 76 00 00 00 06 00 13 54 4c 2d 58	v... ..TL-X			
0040	44 52 31 38 36 30 e6 98 93 e5 b1 95 e7 89 88 00		DR1860..			
0050	0b 00 03 21 2e 20 00 07 00 01 01 00 05 00 11 4c		1 0	r		

实验结果与分析

实验分析：

- 目的MAC地址： ff:ff:ff:ff:ff:ff
- 源MAC地址： f4:2a:7d:57:29:ad
- 类型： 0x0800，上层协议为IPv4协议
- 数据字段： 可见字节长度为160字节，包含IPv4头部、UDP头部和UDP payload数据。
- FCS： 不可见

实验结果与分析

绘制以太网帧格式：

目的MAC地址	源MAC地址	帧内封装的上层协议类型	数据	FCS
ff:ff:ff:ff:ff:ff	f4:2a:7d:57:29:ad	IPv4 (0x0800)	160字节	不可见

主要内容

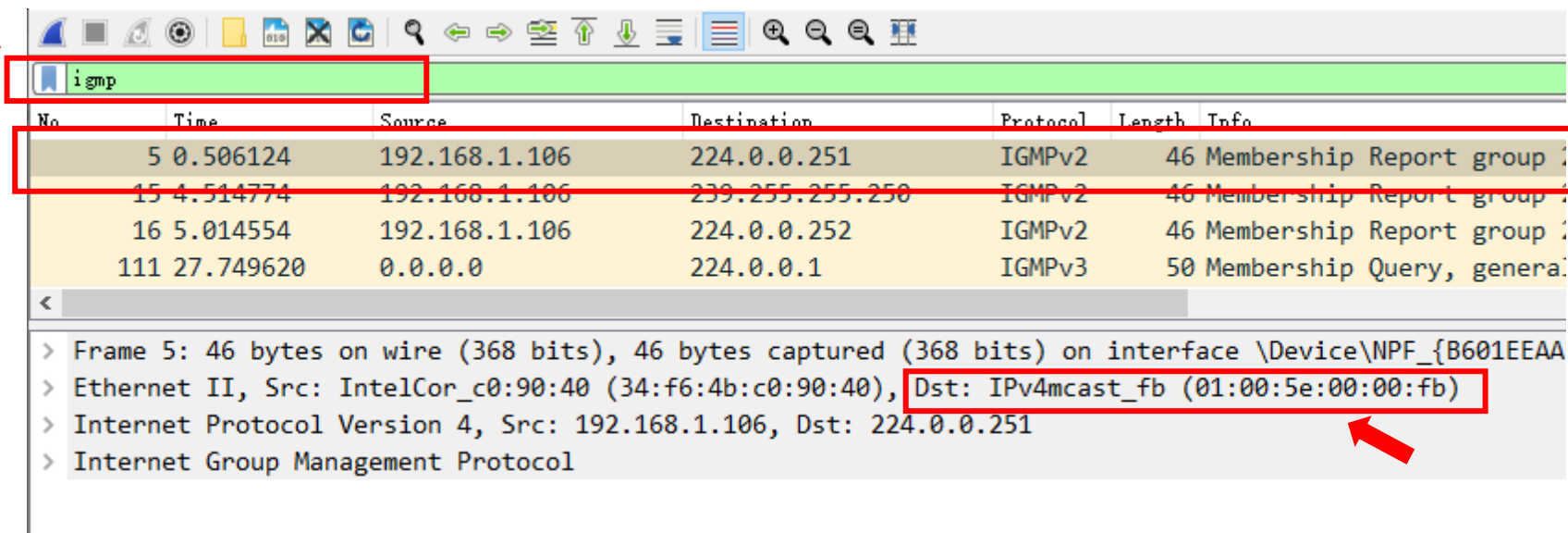
- 一、实验原理
- 二、单播帧抓包实验
- 三、广播帧抓包实验
- 四、多播帧抓包实验

多播帧抓包实验实例

7、使用因特网组管理协议 (IGMP, Internet Group Management Protocol) 对捕获的数据包进行筛选。过滤表达式如下: **igmp**

[IGMP是一个组播协议, 其信息封装在IP数据报中, 它的IP协议号为2。]

8、从中选取任一多播数据包, 观察MAC帧格式, 并进行分析。



The screenshot shows the Wireshark network protocol analyzer interface. The filter bar at the top contains the filter **igmp**. The packet list pane shows several captured packets, with packet 5 selected. The packet details pane shows the structure of packet 5: Ethernet II (Src: IntelCor_c0:90:40, Dst: IPv4mcast_fb (01:00:5e:00:00:fb)), Internet Protocol Version 4 (Src: 192.168.1.106, Dst: 224.0.0.251), and Internet Group Management Protocol (Membership Report group).

No.	Time	Source	Destination	Protocol	Length	Info
5	0.506124	192.168.1.106	224.0.0.251	IGMPv2	46	Membership Report group
15	4.514774	192.168.1.106	239.255.255.250	IGMPv2	46	Membership Report group
16	5.014554	192.168.1.106	224.0.0.252	IGMPv2	46	Membership Report group
111	27.749620	0.0.0.0	224.0.0.1	IGMPv3	50	Membership Query, general

Frame 5: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{B601EEAA...}
Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.1.106, Dst: 224.0.0.251
Internet Group Management Protocol

[Ethernet中一部分物理地址 (MAC地址) 被保留用于多播, 即从 01:00:5e:00:00:00到01:00:5e:7f:ff:ff。]

实验结果与分析

实验结果:

No.	Time	Source	Destination	Protocol	Length	Info
5	0.506124	192.168.1.106	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.
<						
> Frame 5: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{B601EEAA-316D-44}						
v Ethernet II, Src: IntelCor_c0:90:40 (34:f6:4b:c0:90:40), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)						
v Destination: IPv4mcast_fb (01:00:5e:00:00:fb) ←						
Address: IPv4mcast_fb (01:00:5e:00:00:fb)						
....0. = LG bit: Globally unique address (factory default)						
....1. = IG bit: Group address (multicast/broadcast) ←						
v Source: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)						
Address: IntelCor_c0:90:40 (34:f6:4b:c0:90:40)						
....0. = LG bit: Globally unique address (factory default)						
....0. = IG bit: Individual address (unicast)						
Type: IPv4 (0x0800)						
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 224.0.0.251						
> Internet Group Management Protocol						
<						
0000	01 00 5e 00 00 fb 34 f6 4b c0 90 40 08 00	46 00	..^...4. K..@..F.			
0010	00 20 b3 d3 00 00 01 02 cd f6 c0 a8 01 6a e0 00	 j . .			
0020	00 fb 94 04 00 00 16 00 09 04 e0 00 00 fb				

实验结果与分析

实验分析：

- 目的MAC地址： 01:00:5e:00:00:fb
- 源MAC地址： 34:f6:4b:c0:90:40
- 类型： 0x0800，上层协议为IPv4协议
- 数据字段：可见字节长度为32字节，包含IPv4头部和IGMP信息。
- FCS：不可见

实验结果与分析

绘制以太网帧格式：

目的MAC地址	源MAC地址	帧内封装的上层协议类型	数据	FCS
01:00:5e:00:00:fb	34:f6:4b:c0:90:40	IPv4 (0x0800)	32字节	不可见

