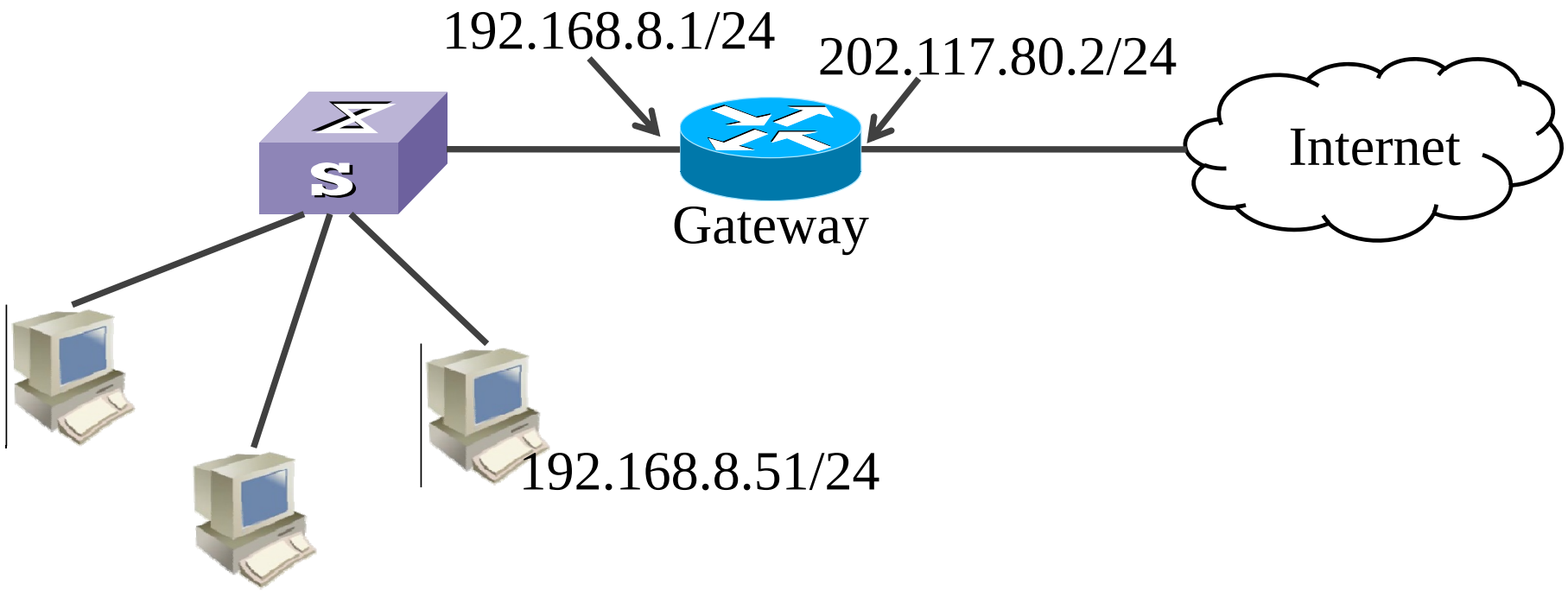
Experiment 4: Parsing IP packets

- Title：Parsing IP packets
- Purpose：By analyzing IP packets, we can understand the working principle of IP, ARP, TCP, HTTP and DNS protocols.

Network topology for experiment



192.168.8.50/24 → http://www.baidu.com

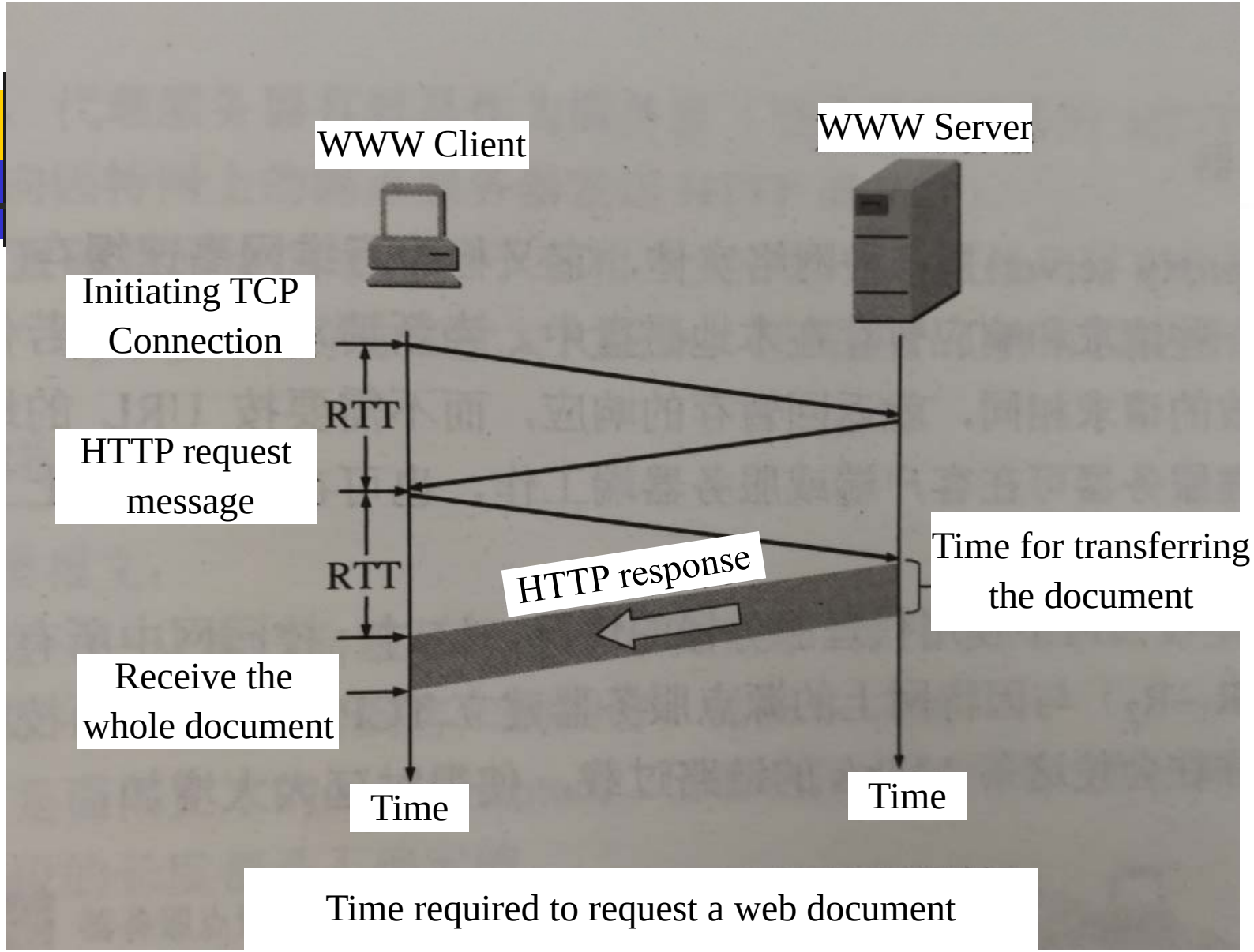
Process of accessing webpage

- **Access http://www.baidu.com**
- Step 1. DNS → UDP → IP → ARP
  recursion/iteration ↘ ICMP
- Step 2. Establish TCP connection by three-way handshake.
- Step 3. Client sends HTTP request.
- Step 4. Server receive and return HTTP response.
- Step 5. Release TCP connection by four-way wavehand.

HTTP working mode

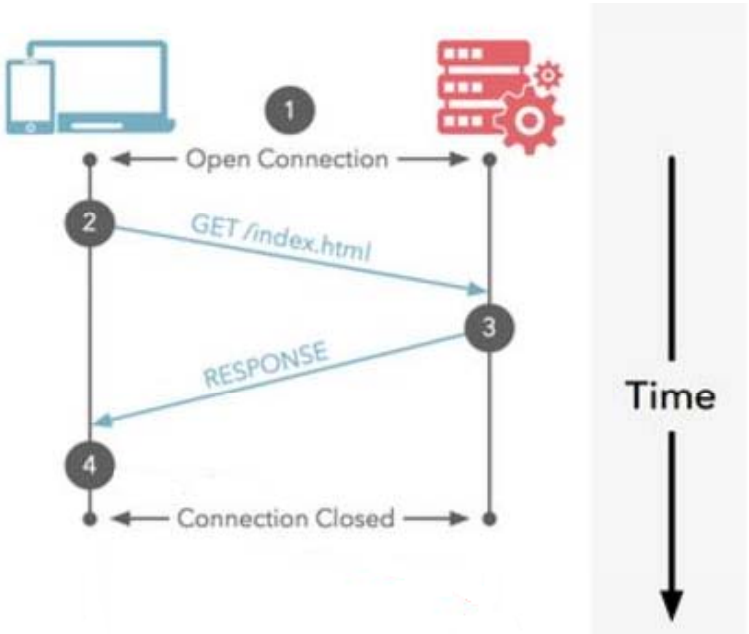
HTTP

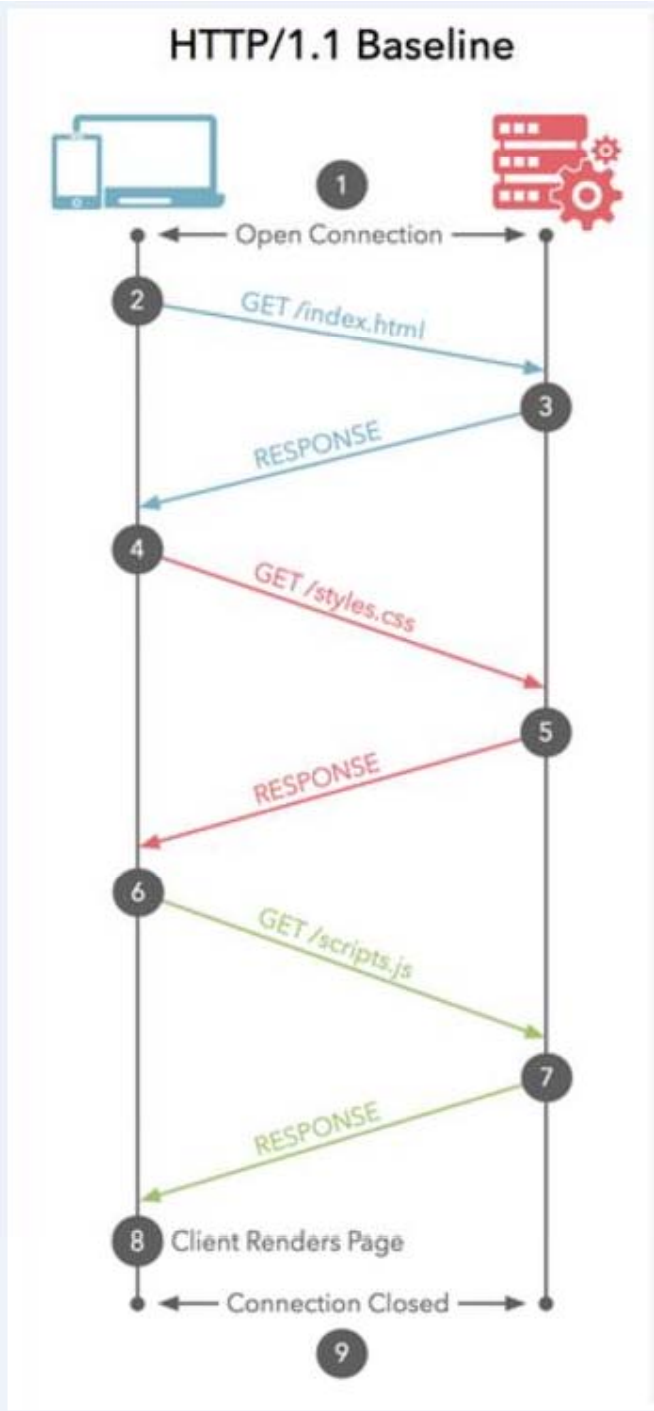
- 1.0: NonPersistent Connection
  - 1 TCP→1 HTTP request/response
- 1.1: Persistent Connection
  - With Pipelining
  - Without Pipelining
  - 1 TCP→ multiple HTTP request/response



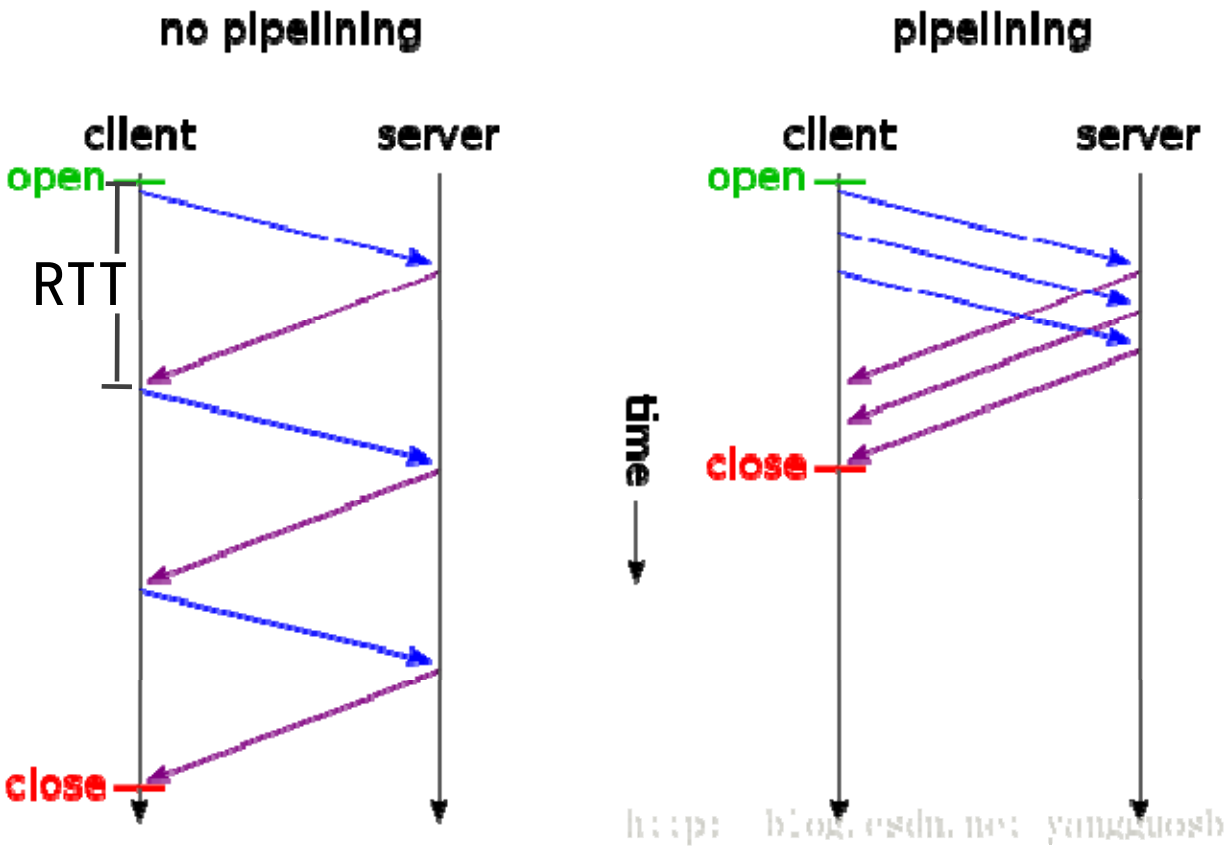
Time required to request a web document

HTTP 1.0


1
Open Connection
2
GET /index.html
3
RESPONSE
4
Connection Closed
Time


HTTP/1.1 Baseline
1
Open Connection
2
GET /index.html
3
RESPONSE
4
GET /styles.css
5
RESPONSE
6
GET /scripts.js
7
RESPONSE
8
Client Renders Page
Connection Closed
9

Pipeline connection



Data encapsulation

DNS request

Frame header	IP Header	UDP Header	DNS Header	DATA	Frame Tail

HTTP request

Frame header	IP Header	TCP Header	HTTP Header	Entity	Frame Tail

ARP message format

Byte	
2	Network type
2	Protocol type
1	Length for PA
1	Length for IP
2	Operation
6	Source PA
4	Source IP
6	Destination PA
4	Destination IP

"1" denote Ether

"0x0800" is IP

PA: Physical address

1—ARP request
2—ARP response
3—RARP request
4—RARP response

Destination PA is empty in the request message

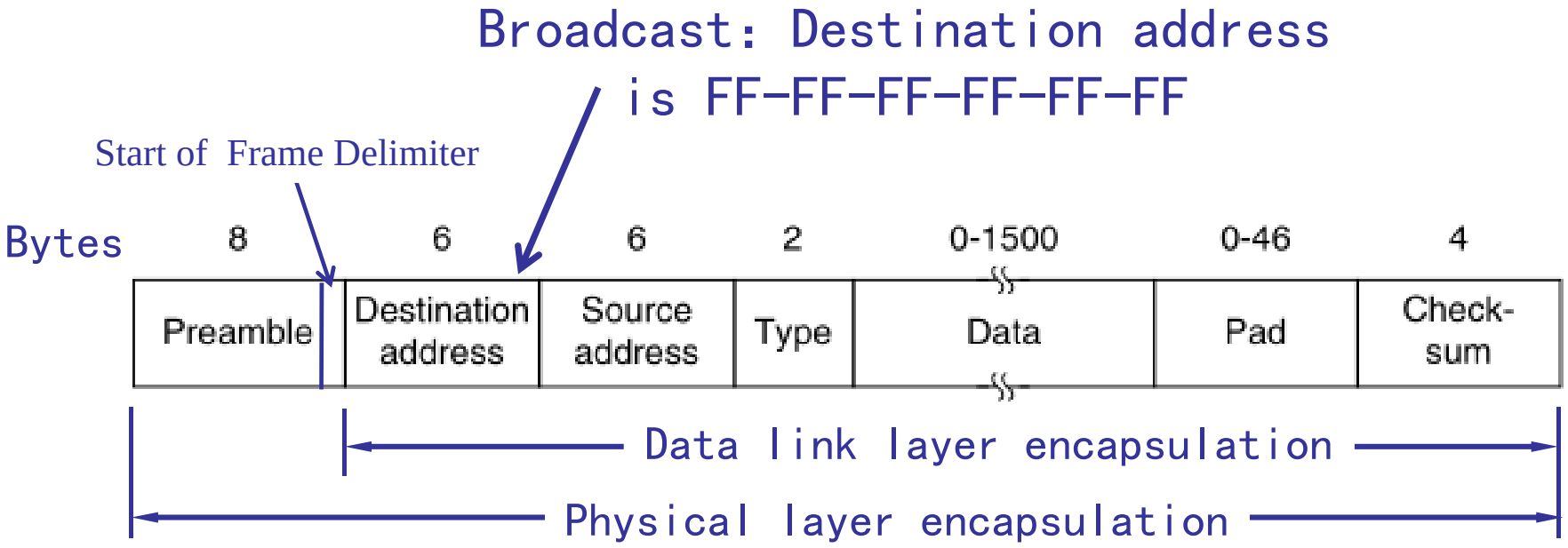
- ARP message is sealed directly in the data field of the MAC frame. The type of MAC is 0806.

Destination address	Source address	Frame type	Data
DA	SA	0806	Whole ARP message

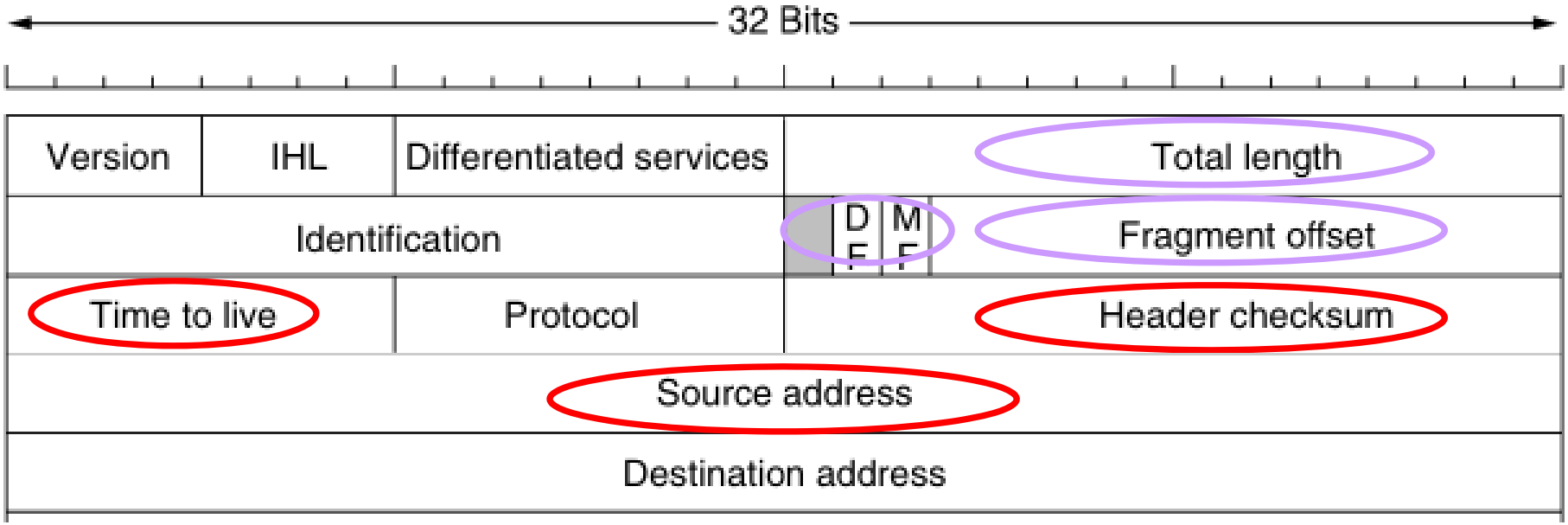
http://blog.csdn.net/

- Commands:
  - arp -d, Clear ARP cache
  - arp -a display ARP cache list

Ethernet frame format



IP Packet Header



When the router forward IP packet in our network setting, which fields of the IP header should be changed?

Tasks for experiment 4

- Catch packets to get the following information:

1. www.baidu.com →IP? (**ipconfig /flushdns**
   ipconfig /displaydns)
2. IP and MAC for gateway?
3. ISN of data？Server ISN(**initialization sequence number**)？
4. HTTP version，working mode？
5. Find one TCP connection, Amount of data sent? Amount of data received ？
6. Describe the process of three-way handshake connection and four-way wavehand release.

Catch packets

1.1 Preliminary

(1) Clear browser cache

Ensure that the Web is caught from network. Chrome: **Options --> Under the Hood --> Clear browsing data**。

(2) Clear DNS cache

Ensure that that the map of domain name and ip is got from network request. In Windows XP， input **ipconfig /flushdns**

(3) Set filter rules

In order to facilitate the analysis， set filter rules before catching the packets. In Filter ToolBar， Enter filter rule normal expression.

(4) Close network applications

1.2 Start Wireshark

Capture --> Interfaces， set interface, click Start

1.3 Input URL in the browser

Such as： http://www.baidu.com， enter。

1.4 Stop catching packets.

Display Filter

Packet List Pane

Packet Details Pane

Dissector Pane

Miscellaneous

Capturing from Microsoft: \Device\NPF_{A9559F22-1504-4F4D-8067-DC61681A9F9C} [Wireshark 1.3.2 (SVN Rev 44520 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.src == 192.168.1.102 or ip.dst == 192.168.1.102 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
953	97.2501200	192.168.1.102	106.187.54.210	TCP	54	imgames > http [ACK] Seq=1277 Ack=5954 Win=4
954	97.2503690	106.187.54.210	192.168.1.102	HTTP	247	HTTP/1.1 200 OK (application/json)
955	97.4460230	192.168.1.102	106.187.54.210	TCP	54	imgames > http [ACK] Seq=1277 Ack=6147 Win=4
956	108.860594	192.168.1.102	199.47.217.148	TCP	66	abbaccuray > http [SYN] Seq=0 Win=8192 Len=0
957	109.011307	199.47.217.148	192.168.1.102	TCP	66	http > abbaccuray [SYN, ACK] Seq=0 Ack=1 Win
958	109.011448	192.168.1.102	199.47.217.148	TCP	54	abbaccuray > http [ACK] Seq=1 Ack=1 Win=1728
959	109.013060	192.168.1.102	199.47.217.148	HTTP	250	GET /subscribe?host_int=274802669&ns_map=126
960	109.026703	199.47.217.148	192.168.1.102	TCP	54	http > abbaccuray [RST, ACK] Seq=1 Ack=197 W
961	109.027505	199.47.217.148	192.168.1.102	TCP	54	http > abbaccuray [RST, ACK] Seq=1461 Ack=19
962	109.027764	199.47.217.148	192.168.1.102	TCP	54	http > abbaccuray [RST, ACK] Seq=4381 Ack=19
963	109.028324	199.47.217.148	192.168.1.102	TCP	54	http > abbaccuray [RST] Seq=1 Win=1665536 Le
964	109.030555	192.168.1.102	199.47.217.148	TCP	66	laplink > http [SYN] Seq=0 Win=8192 Len=0 MS

```
Frame 963: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Tp-LinkT_74:bf:3a (b0:48:7a:74:bf:3a), Dst: Prodrive_26:12:bf (00:0f:11:26:12:bf)
Internet Protocol Version 4, Src: 199.47.217.148 (199.47.217.148), Dst: 192.168.1.102 (192.168.1.102)
Transmission Control Protocol, Src Port: http (80), Dst Port: abbaccuray (1546), Seq: 1, Len: 0
```

```
0000  00 0f 11 26 12 bf b0 48  7a 74 bf 3a 08 00 45 00   ...&...H zt.:..E.
0010  00 28 62 6b 00 00 55 06  a0 92 c7 2f d9 94 c0 a8   .(bk..U. .../....
0020  01 66 00 50 06 0a 47 a2  b7 02 00 00 00 00 50 04   .f.P..G. ......P.
0030  0c b5 3b 5a 00 00                                  ..;Z..
```

Microsoft: \Device\NPF_{A9559F22-1504-... | Packets: 4598 Displayed: 4163 Marked: 0 | Profile: Default