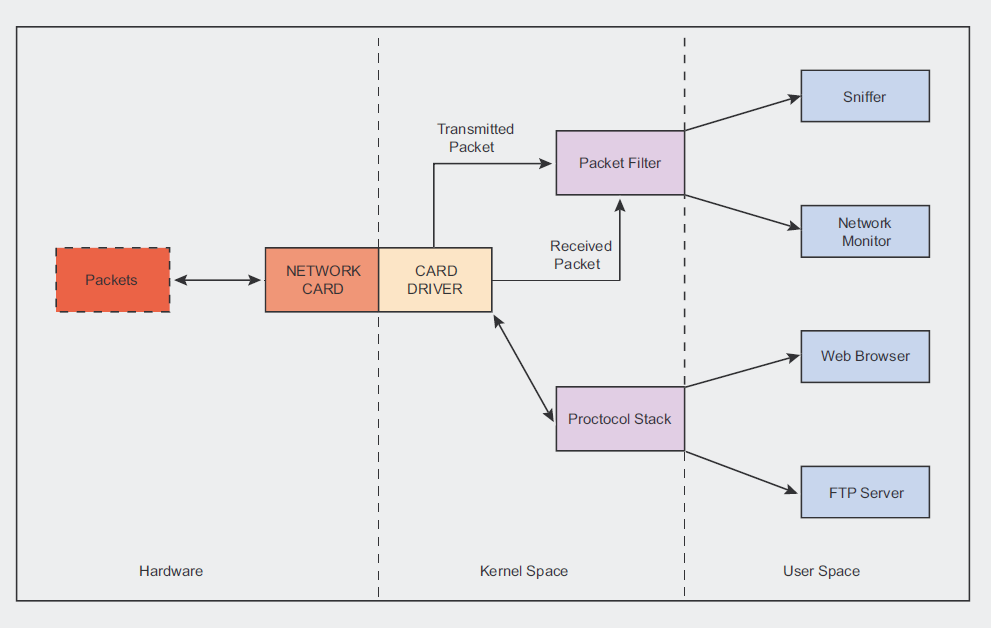
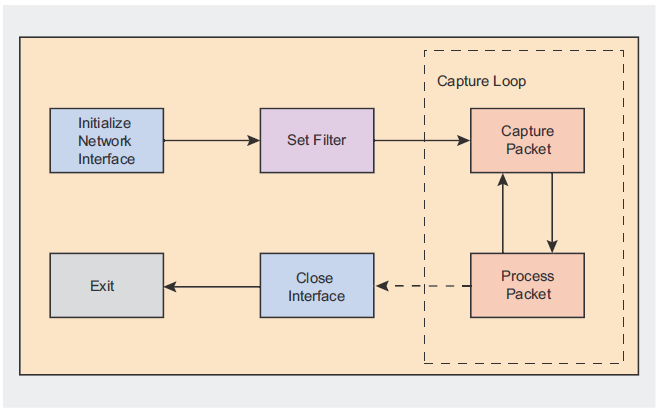
网络嗅探器

捕获数据包过程



编写网络嗅探器的流程



仅做分析

1）打开设备（pcap\_open\_live）

2）设置过滤器（pcap\_compile、pcap\_setfilter）

3）For循环：

a）抓取报文（pcap\_next）

b）报文解析

4）关闭设备（pcap\_close）

1）打开设备（pcap\_open\_live, libnet\_init）

2）设置过滤器（pcap\_compile、pcap\_setfilter）

3）For循环：

a）抓取报文（pcap\_next）

b）报文解析

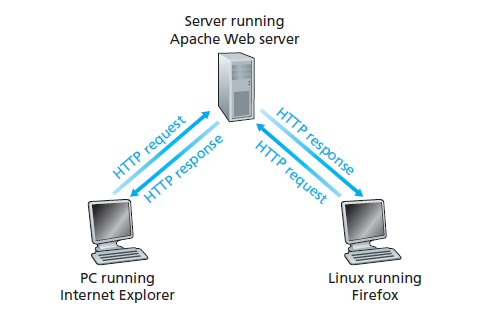
c）内容匹配

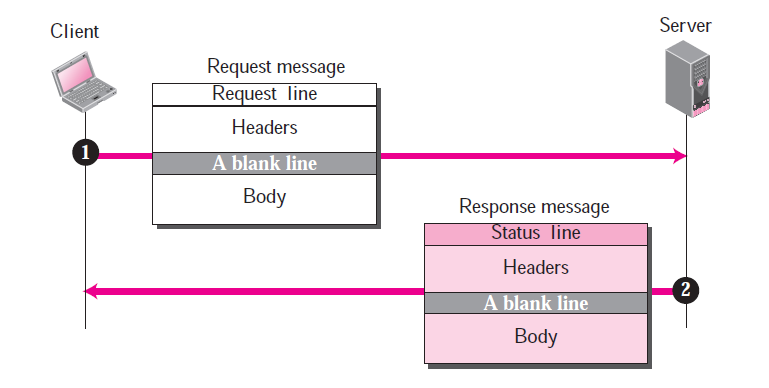
d）伪造响应报文（libnet\_build\_xxx）

e）发送响应报文（libnet\_write、libnet\_clear\_packet）

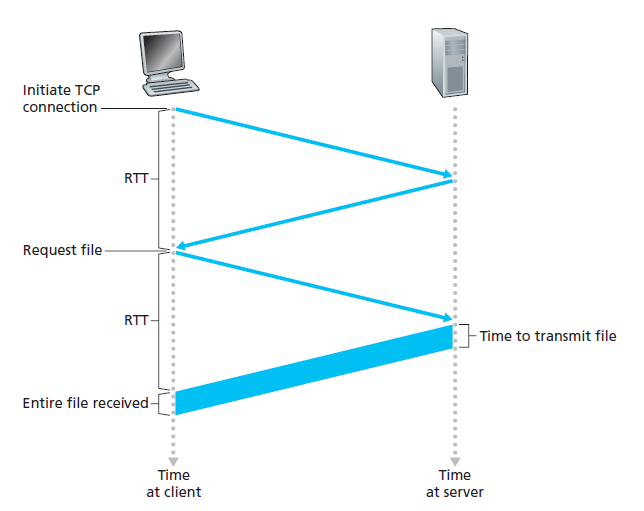
4）关闭设备（pcap\_close、libnet\_destroy）

HTTP的请求-响应行为：





请求并接收一个HTML文件所需的时间估算



典型的HTTP请求报文：

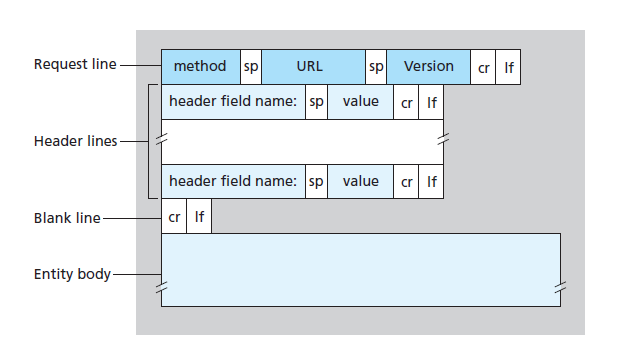
GET /somedir/page.html HTTP/1.1

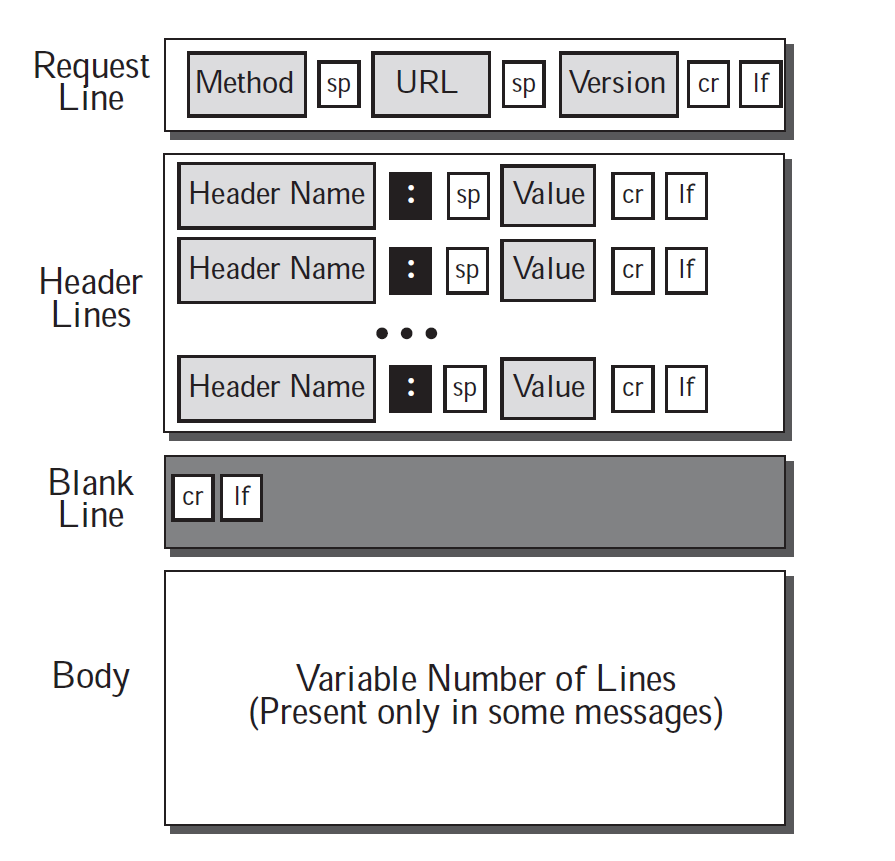
Host: www.someschool.edu

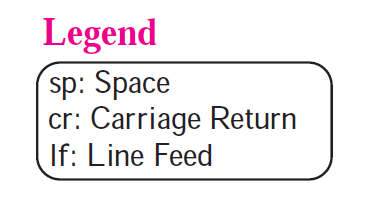
Connection: close

User-agent: Mozilla/5.0

Accept-language: fr







HTTP/1.1 200 OK

Connection: close

Date: Tue, 09 Aug 2011 15:44:04 GMT

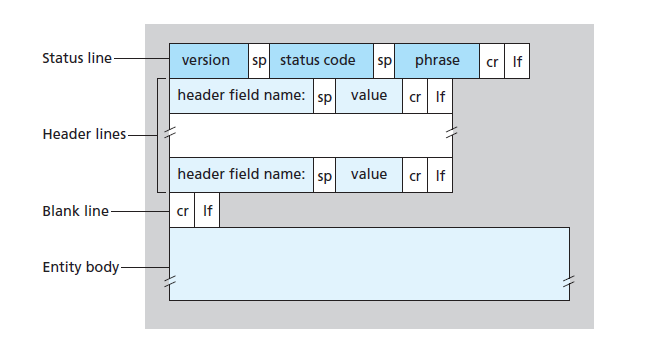
Server: Apache/2.2.3 (CentOS)

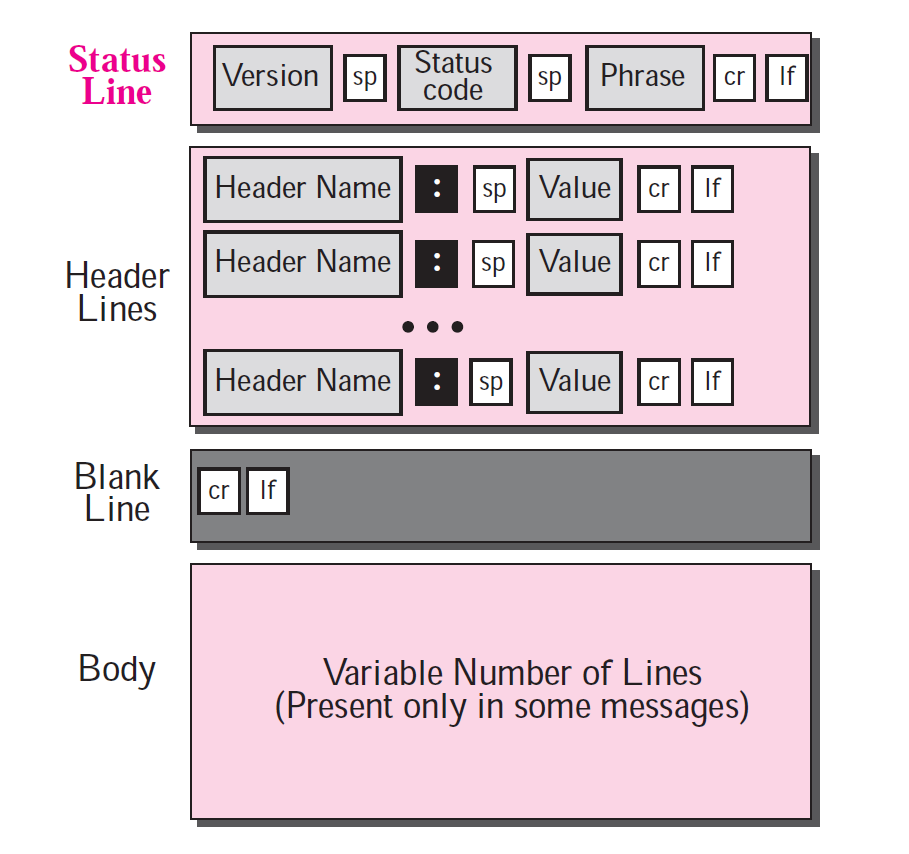
Last-Modified: Tue, 09 Aug 2011 15:11:03 GMT

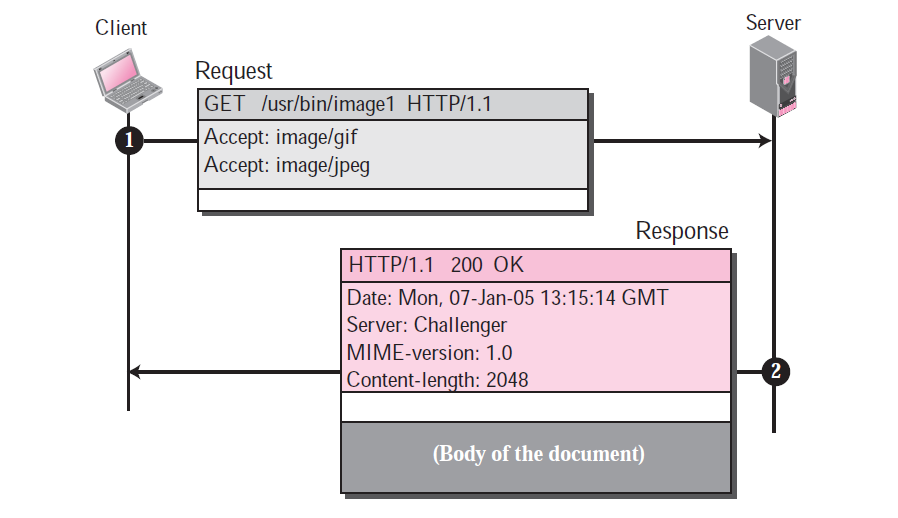
Content-Length: 6821

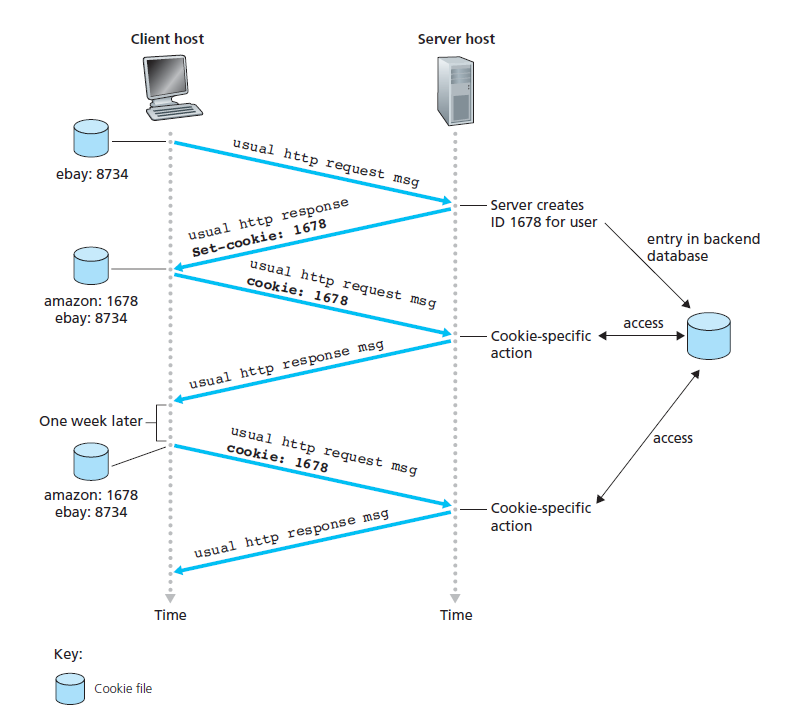
Content-Type: text/html

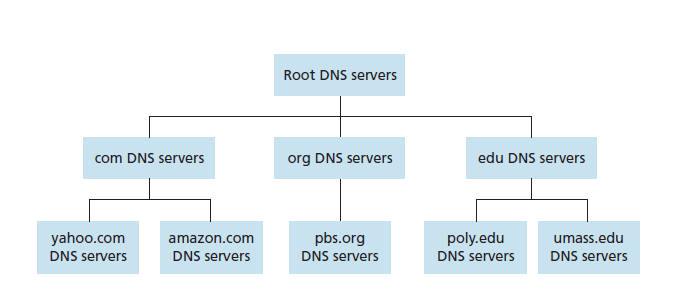
(datadatadatadatadata ...)





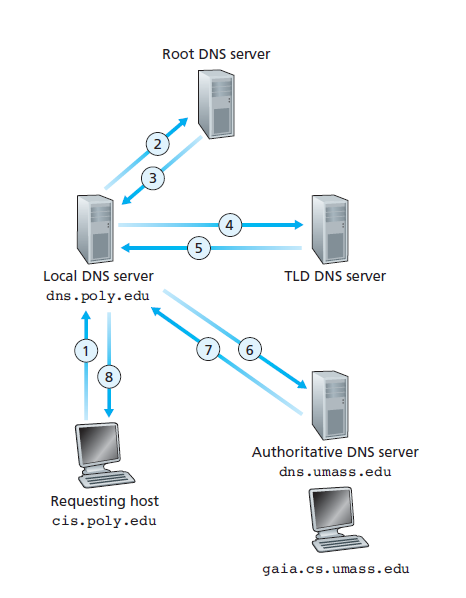






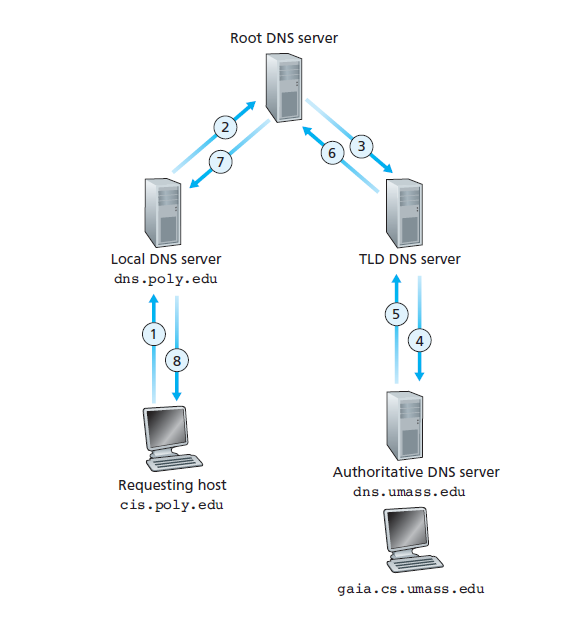
DNS服务实现方式：分布式、层次数据库。

DNS分类：根DNS服务器，顶级域DNS服务器，权威DNS服务器。本地DNS服务器，每个ISP都有一台本地DNS服务器。

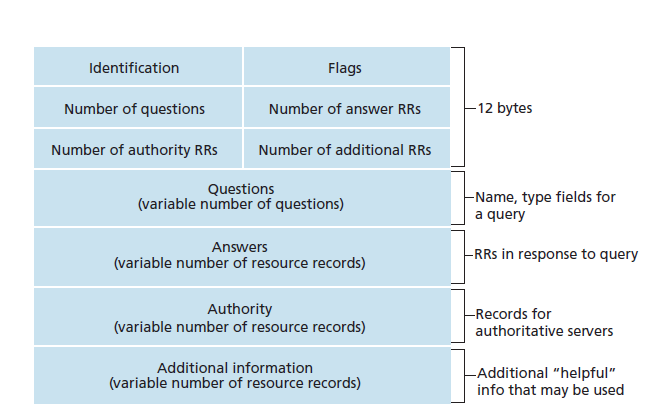


一个简单的域名查找过程：cis.poly.edu访问gaia.cs.umass.edu。

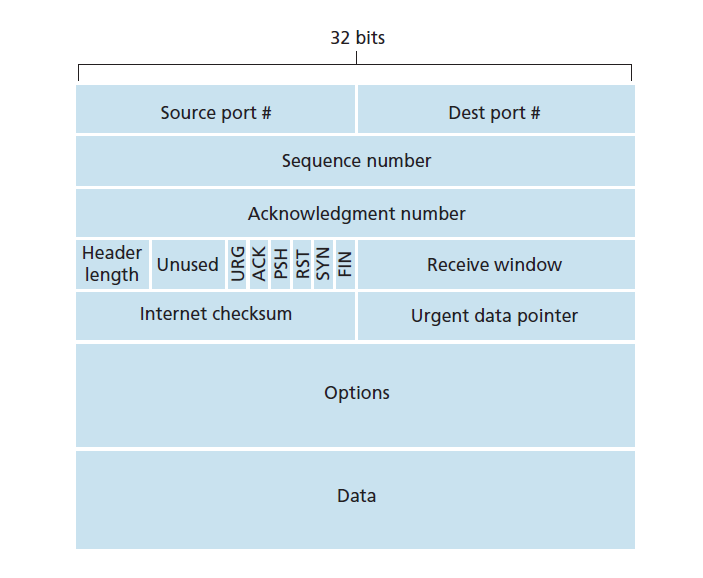
DNS查询方式：递归查询和迭代查询（cis.poly.edu到dns.poly.edu是递归查询），后继3个查询是迭代查询。任何DNS查询既可以是迭代的也可以是递归的。

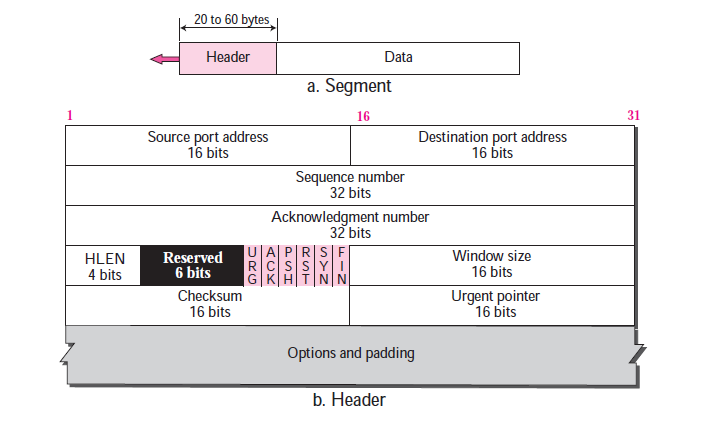


一个完全的递归式的查询。

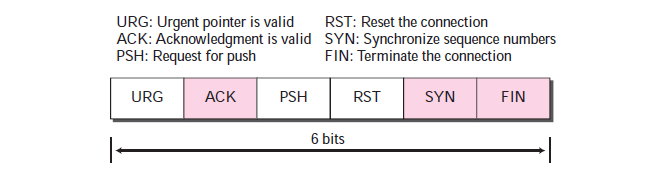


DNS报文格式。

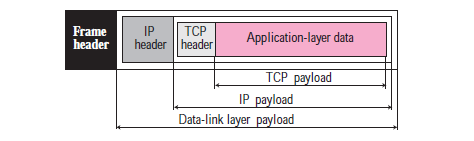




TCP报头格式



TCP flag



网络报文

构造TCP server数据响应报文（已建立连接）

TCP client的数据请求报文request

TCP server的数据响应报文response

response.tcphdr.src\_port = request.tcphdr.dst\_port;

response.tcphdr.dst\_port = request.tcphdr.src\_port;

response.tcphdr.seq\_no = request.tcphdr.ack\_no;

response.tcphdr.ack\_no = request.tcphdr.seq\_no + request.tcphdr.payload\_len;

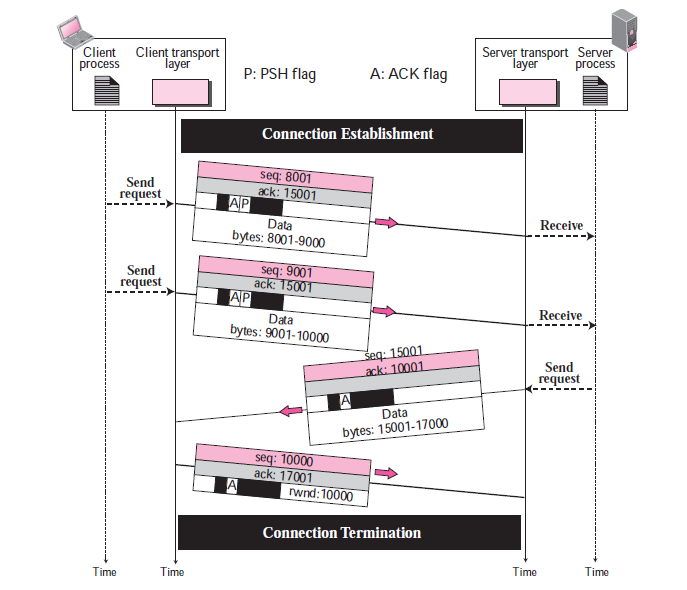
request.tcphdr.payload\_len = request.iphdr.total\_len - request.iphdr.hdr\_len - request.tcphdr.hdr\_len;

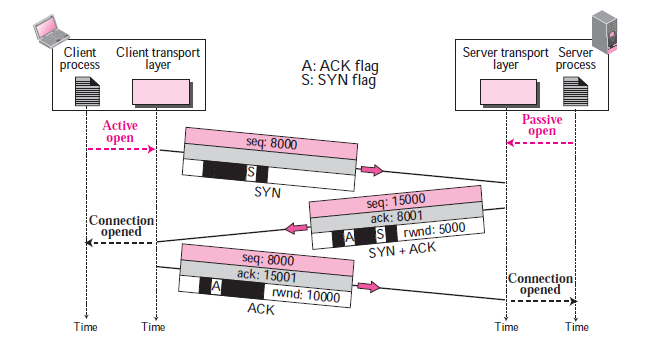
response.tcphdr.flag = TH\_ACK;

（RST报文的话response.tcphdr.flag = TH\_RST）;

（如果响应报文带数据并且需要快速推送到应用层的话，response.tcphdr.flag |= TH\_PSH）;

（如果响应报文是最后一个报文，即服务端打算主动关闭连接的话，response.tcphdr.flag |= TH\_FIN）；





构造TCP server建立连接握手响应报文（第二个报文）

response.tcphdr.src\_port = request.tcphdr.dst\_port;

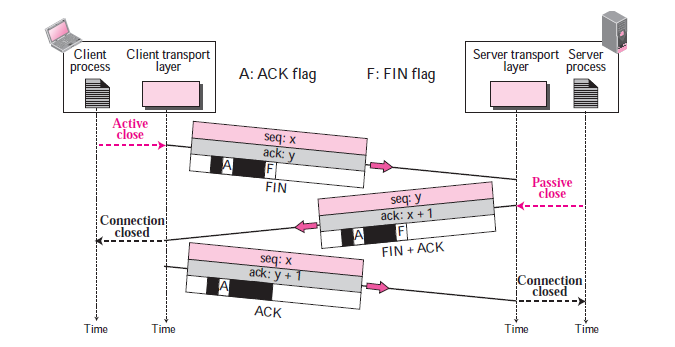
response.tcphdr.dst\_port = request.tcphdr.src\_port;

response.tcphdr.seq\_no = any;

response.tcphdr.ack\_no = request.tcphdr.seq\_no + 1;

response.tcphdr.flag = TH\_SYN | TH\_ACK;

（RST报文的话response.tcphdr.flag = TH\_RST | TH\_ACK）;



构造TCP server关闭连接握手响应报文（第二个报文）

response.tcphdr.src\_port = request.tcphdr.dst\_port;

response.tcphdr.dst\_port = request.tcphdr.src\_port;

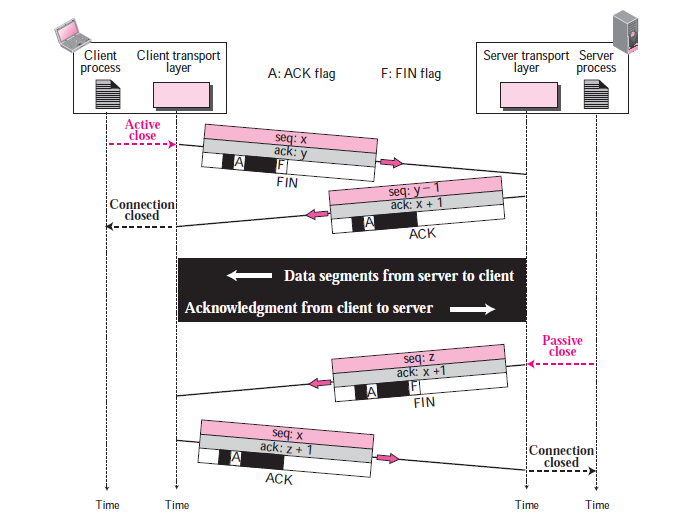
response.tcphdr.seq\_no = request.tcphdr.ack\_no;

response.tcphdr.ack\_no = request.tcphdr.seq\_no + 1;

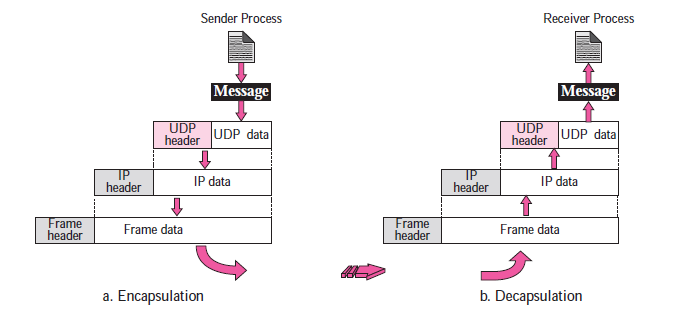
response.tcphdr.flag = TH\_FIN | TH\_ACK;

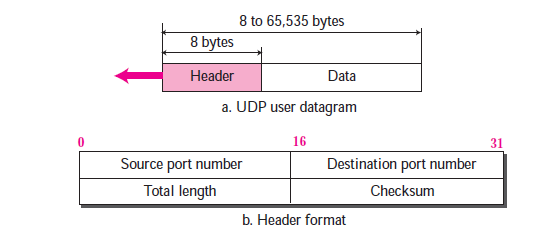
（RST报文的话response.tcphdr.flag = TH\_RST | TH\_ACK）;

半关闭连接



UDP打包和解包过程





UDP报头格式

构造UDP server数据响应报文

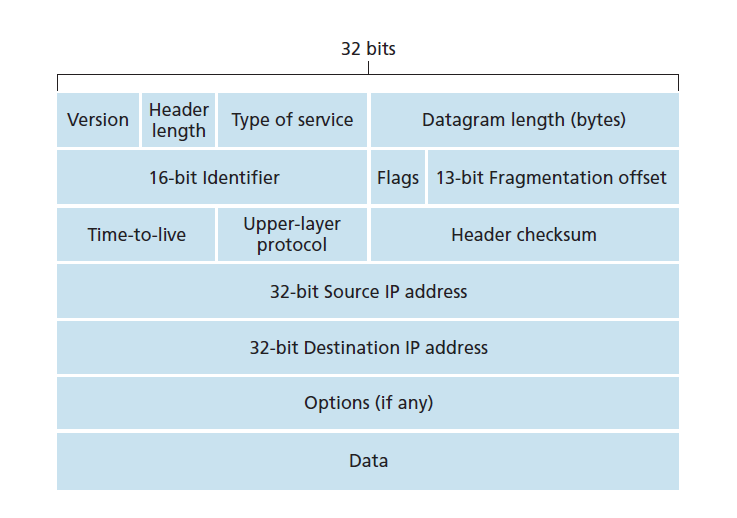
UDP client的数据请求报文request

UDP server的数据响应报文response

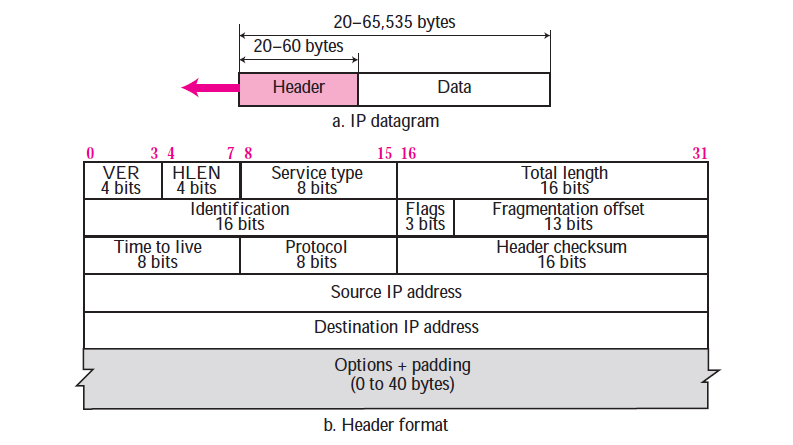
response.udphdr.src\_port = request.udphdr.dst\_port;

response.udphdr.dst\_port = request.udphdr.src\_port;

response.udphdr.total\_len = response.udphdr.payload\_len + 8;



IP报文格式



IP报头格式

构造IP server数据响应报文

IP client的数据请求报文request

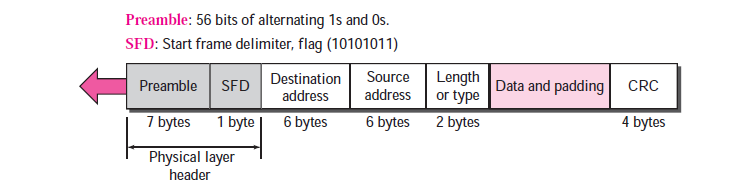
IP server的数据响应报文response

response.iphdr.src\_addr = request.iphdr.dst\_addr;

response.iphdr.dst\_addr = request.iphdr.src\_addr;

response.iphdr.total\_len = response.iphdr.hdr\_len + response.transport.hdr\_len + response.application.payload\_len;

response.iphdr.protocol = request.iphdr.protocol;



以太网帧格式

构造Ethernet server数据响应报文

Ethernet client的数据请求报文request

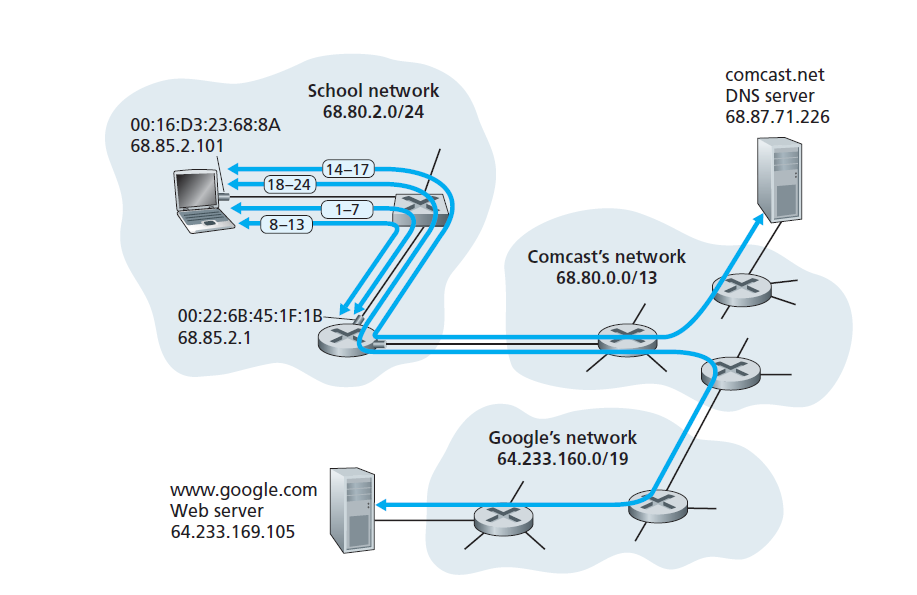
Ethernet server的数据响应报文response

response.ethhdr.src\_mac = request.ethhdr.dst\_mac;

response.ethhdr.dst\_mac = request.ethhdr.src\_mac;

response.ethhdr.payload\_len = response.iphdr.total\_len;

response.ethhdr.ether\_type= request.ethhdr. ether\_type;



场景：一名学生Bob使用笔记本，从学校的以太网接入，学校内使用的所有IP地址都在comcast地址块中，访问Web页面（比如www.google.com）。

访问web页面过程:

1-7）DHCP过程：

（1）Bob的笔记本上的操作系统构造包含DHCP请求的UDP/IP报文：

request.udphdr.src\_port = 68;

request.udphdr.dst\_port = 67;

request.iphdr.src\_addr = 0.0.0.0;

request.iphdr.dst\_addr = 255.255.255.255;

（2）网卡驱动将包含DHCP请求的IP数据报封装到以太网帧中：

reqeust.ethhdr.src\_mac = 00:16:D3:23:68:8A；（笔记本网卡MAC地址）

reqeust.ethhdr.dst\_mac = FF: FF: FF: FF: FF:FF；

（3）包含DHCP请求的广播以太网帧是第一个由Bob的笔记本发送到以太网交换机的帧，该交换机在所有的出端口广播该帧，该帧被广播到整个68.85.2.0/24子网；

（4）路由器68.85.2.1在接口00:22:6B:45:1F:1B收到包含DHCP请求的广播以太网帧，并逐级解析出HDCP请求报文；

（5）运行在路由器68.85.2.1上的DHCP服务器接受并处理HDCP请求报文，DHCP服务器以CIDR块68.85.2.0/24分配IP地址，DHCP服务器将IP地址68.85.2.101分配给Bob的笔记本，并构造DHCP响应报文，DHCP响应报文包含：a.分配给在Bob的笔记本的IP地址68.85.2.101，b.DNS服务器的IP地址68.87.71.226，c.默认网关路由器的IP地址68.85.2.1，d.子网块掩码68.85.2.0/24，并将DHCP响应报文封装在UDP/IP报文中，最终封装到以太网帧中发送出去：

response.udphdr.src\_port = 67;

response.udphdr.dst\_port = 68;

response.iphdr.src\_addr = 68.85.2.1;

response.iphdr.dst\_addr = 255.255.255.255;

reqeust.ethhdr.src\_mac = 00:22:6B:45:1F:1B；

reqeust.ethhdr.dst\_mac = 00:16:D3:23:68:8A；（笔记本网卡MAC地址）

（6）包含DHCP响应的以太网帧通过交换机发送到Bob的笔记本；

（7）Bob的笔记本接收到包含DHCP响应的以太网帧，逐层解析，并提取出DHCP响应报文内容，并初始化网络组件。

8-13）ARP过程：

14-17）DNS解析过程：

18-24）HTTP解析过程：