互联网协议实验报告

热伊莱·图尔贡　2018K8009929030

一、 实验题目

互联网协议实验

二、 实验内容

1. 在节点 h1 上开启 Wireshark 抓包，用 wget 下载 www.ucas.ac.cn 页面；
2. 调研说明 wireshark 抓到的几种协议（ARP, DNS, TCP, HTTP, HTTPS）
3. 调研解释 h1 下载 ucas 页面的整个过程（几种协议的运行机制）

三、 实验流程

1. 终端运行 sudo mn –nat 指令，将 hosts 连接到互联网；
2. 启动 mininet 程序后，运行 xterm h1 指令，打开控制 h1 的终端；
3. 在 h1 终端中运行 echo “nameserver 1.2.4.8”> /etc/resolv.conf；
4. 在 h1 终端中运行 wireshark &，启动 wireshark 抓包程序；
5. 在 GUI 界面中选择 h1-eth0，开始抓包；
6. 在 h1 终端中运行 wget www.ucas.ac.cn 下载国科大主页；
7. 调研分析获取到的几种互联网协议；
8. 调研解释 h1 下载 ucas 页面的整个过程

四、 实验结果

1. 抓包结果：

No.	Time	Source	Destination	Protocol	Length	Info
5	1.823394435	fe80::7879:d7ff:fe2…	ff02::fb	MDNS	107	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR…
6	34.896633401	a2:a2:c5:07:61:9c	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
7	34.896758154	0a:11:6c:73:e9:4c	a2:a2:c5:07:61:9c	ARP	42	10.0.0.3 is at 0a:11:6c:73:e9:4c
8	34.896760208	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x51df A www.ucas.ac.cn
9	34.896810251	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x56dd AAAA www.ucas.ac.cn
10	34.933762067	1.2.4.8	10.0.0.1	DNS	102	Standard query response 0x56dd AAAA www.ucas.ac.cn AAAA 2400:…
11	39.899734098	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x51df A www.ucas.ac.cn
12	39.918263434	1.2.4.8	10.0.0.1	DNS	90	Standard query response 0x51df A www.ucas.ac.cn A 124.16.79.3
13	39.918421243	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x56dd AAAA www.ucas.ac.cn
14	39.933130403	1.2.4.8	10.0.0.1	DNS	102	Standard query response 0x56dd AAAA www.ucas.ac.cn AAAA 2400:…
15	39.933381989	10.0.0.1	124.16.79.3	TCP	74	46894 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 T…
16	39.957921670	124.16.79.3	10.0.0.1	TCP	58	80 → 46894 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
17	39.957966491	10.0.0.1	124.16.79.3	TCP	54	46894 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
18	39.958140513	10.0.0.1	124.16.79.3	HTTP	195	GET / HTTP/1.1
19	39.958382367	124.16.79.3	10.0.0.1	TCP	54	80 → 46894 [ACK] Seq=1 Ack=142 Win=65535 Len=0
20	39.964577783	124.16.79.3	10.0.0.1	HTTP	381	HTTP/1.1 302 Moved Temporarily (text/html)
21	39.964591519	10.0.0.1	124.16.79.3	TCP	54	46894 → 80 [ACK] Seq=142 Ack=328 Win=42013 Len=0

2. ARP 协议：

No.	Time	Source	Destination	Protocol	Length	Info
7	59.391259856	fe80::5cbc:81ff:fef…	ff02::2	ICMPv6	70	Router Solicitation from 5e:bc:81:fd:8f:59
8	100.685566489	42:cb:fb:07:bd:3d	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
9	100.685692759	5e:bc:81:fd:8f:59	42:cb:fb:07:bd:3d	ARP	42	10.0.0.3 is at 5e:bc:81:fd:8f:59
10	100.685694680	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x10d6 A www.ucas.ac.cn
11	100.685753324	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x35d0 AAAA www.ucas.ac.cn
12	100.705901270	1.2.4.8	10.0.0.1	DNS	90	Standard query response 0x10d6 A www.ucas.ac.cn A 124.16.79.3
13	100.906603253	1.2.4.8	10.0.0.1	DNS	102	Standard query response 0x35d0 AAAA www.ucas.ac.cn AAAA 2400:…
14	100.908453261	10.0.0.1	124.16.79.3	TCP	74	46892 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 T…
15	100.926290320	124.16.79.3	10.0.0.1	TCP	58	80 → 46892 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
16	100.926308144	10.0.0.1	124.16.79.3	TCP	54	46892 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
17	100.926649475	10.0.0.1	124.16.79.3	HTTP	195	GET / HTTP/1.1

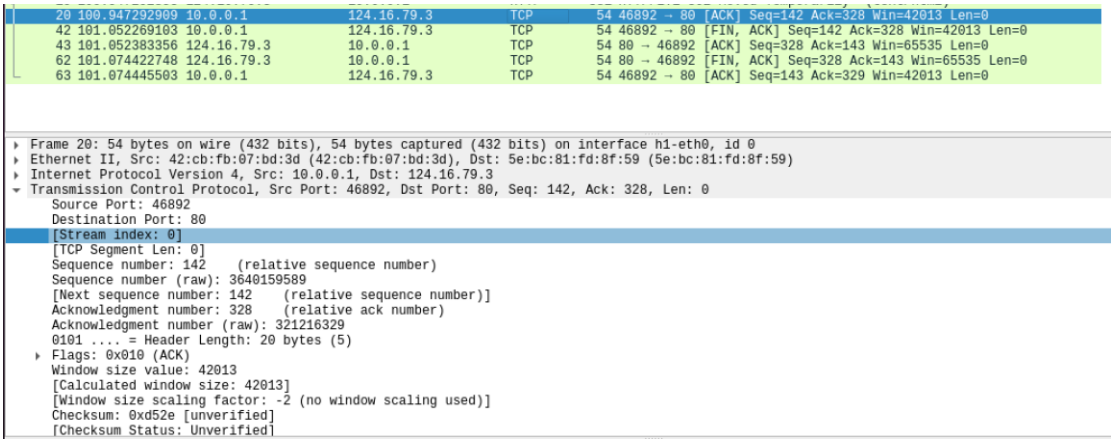
```
▸ Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface h1-eth0, id 0
▾ Ethernet II, Src: 5e:bc:81:fd:8f:59 (5e:bc:81:fd:8f:59), Dst: 42:cb:fb:07:bd:3d (42:cb:fb:07:bd:3d)
  ▸ Destination: 42:cb:fb:07:bd:3d (42:cb:fb:07:bd:3d)
  ▸ Source: 5e:bc:81:fd:8f:59 (5e:bc:81:fd:8f:59)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 5e:bc:81:fd:8f:59 (5e:bc:81:fd:8f:59)
    Sender IP address: 10.0.0.3
    Target MAC address: 42:cb:fb:07:bd:3d (42:cb:fb:07:bd:3d)
    Target IP address: 10.0.0.1
```

3. DNS 协议：

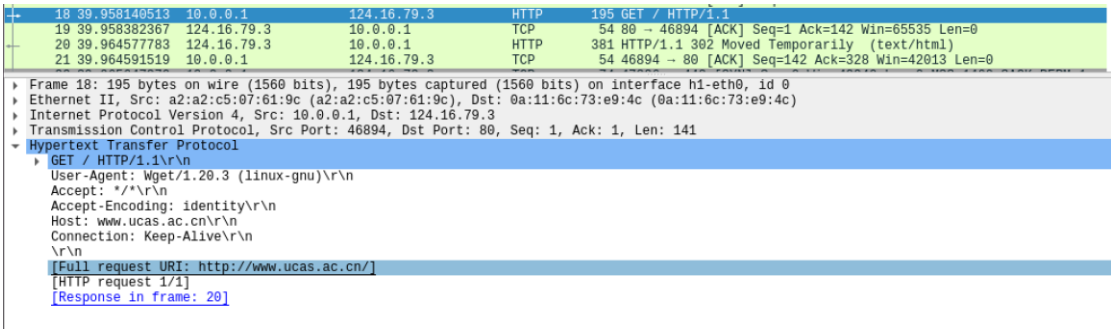
No.	Time	Source	Destination	Protocol	Length	Info
7	59.391259856	fe80::5cbc:81ff:fef…	ff02::2	ICMPv6	70	Router Solicitation from 5e:bc:81:fd:8f:59
8	100.685566489	42:cb:fb:07:bd:3d	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.1
9	100.685692759	5e:bc:81:fd:8f:59	42:cb:fb:07:bd:3d	ARP	42	10.0.0.3 is at 5e:bc:81:fd:8f:59
10	100.685694680	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x10d6 A www.ucas.ac.cn
11	100.685753324	10.0.0.1	1.2.4.8	DNS	74	Standard query 0x35d0 AAAA www.ucas.ac.cn
12	100.705901270	1.2.4.8	10.0.0.1	DNS	90	Standard query response 0x10d6 A www.ucas.ac.cn A 124.16.79.3
13	100.906603253	1.2.4.8	10.0.0.1	DNS	102	Standard query response 0x35d0 AAAA www.ucas.ac.cn AAAA 2400:…
14	100.908453261	10.0.0.1	124.16.79.3	TCP	74	46892 → 80 [SYN] Seq=0 Win=42340 Len=0 MSS=1460 SACK_PERM=1 T…
15	100.926290320	124.16.79.3	10.0.0.1	TCP	58	80 → 46892 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
16	100.926308144	10.0.0.1	124.16.79.3	TCP	54	46892 → 80 [ACK] Seq=1 Ack=1 Win=42340 Len=0
17	100.926649475	10.0.0.1	124.16.79.3	HTTP	195	GET / HTTP/1.1

```
▸ Frame 12: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface h1-eth0, id 0
▾ Ethernet II, Src: 5e:bc:81:fd:8f:59 (5e:bc:81:fd:8f:59), Dst: 42:cb:fb:07:bd:3d (42:cb:fb:07:bd:3d)
  ▸ Destination: 42:cb:fb:07:bd:3d (42:cb:fb:07:bd:3d)
  ▸ Source: 5e:bc:81:fd:8f:59 (5e:bc:81:fd:8f:59)
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 1.2.4.8, Dst: 10.0.0.1
▸ User Datagram Protocol, Src Port: 53, Dst Port: 53189
▸ Domain Name System (response)
```

4. TCP 协议：



5. HTTP 协议：



6. wget 下载的网页

五、 实验分析

1. 互联网数据传输过程中在不同层次使用了不同的协议，主要协议有：ARP 协议，DNS 协议，TCP 协议，HTTP 协议；

2. DNS 协议的封装层次：Ethernet < IP < UDP < DNS；

3. HTTP 协议的封装层次：Ethernet < IP < TCP < HTTP；

4. TCP 协议承载 HTTP 协议；

六、 调研解释

1. ARP 协议：

地址解析协议（英语：Address Resolution Protocol，缩写：ARP）是一个通过解析网络层地址来找寻数据链路层地址的网络传输协议。
在以太网协议中规定，同一局域网中的一台主机要和另一台主机进行直接通信，必须要知道目标主机的 MAC 地址。而在 TCP/IP 协议中，网络层和传输层只关心目标主机的 IP 地址。这就导致在以太网中使用 IP 协议时，数据链路层的以太网协议接到上层 IP 协议提供的数据中，只包含目的主机的 IP 地址。于是需要一种方法，根据目的主机的 IP 地址，获得其 MAC 地址。这就是

ARP 协议要做的事情。所谓地址解析（address resolution）就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。[i]

2. DNS 协议：

域名系统（英语：Domain Name System，缩写：DNS）是互联网的一项服务。它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。
举一个例子，zh.wikipedia.org 作为一个域名就和 IP 地址 198.35.26.96 相对应。DNS 就像是一个自动的电话号码簿，我们可以直接拨打 198.35.26.96 的名字 zh.wikipedia.org 来代替电话号码（IP 地址）。DNS 在我们直接调用网站的名字以后就会将像 zh.wikipedia.org 一样便于人类使用的名字转化成像 198.35.26.96 一样便于机器识别的 IP 地址。[ii]

3. TCP 协议：

传输控制协议（英语：Transmission Control Protocol，缩写：TCP）是一种面向连接的、可靠的、基于字节流的传输层通信协议。
在因特网协议族（Internet protocol suite）中，TCP 层是位于 IP 层之上，应用层之下的中间层。不同主机的应用层之间经常需要可靠的、像管道一样的连接，但是 IP 层不提供这样的流机制，而是提供不可靠的包交换。
应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流，然后 TCP 把数据流分割成适当长度的报文段（通常受该计算机连接的网络的数据链路层的最大传输单元（MTU）的限制）。之后 TCP 把结果包传给 IP 层，由它来透过网络将包传送给接收端实体的 TCP 层。TCP 为了保证不发生丢包，就给每个包一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的包发回一个相应的确认信息（ACK）；如果发送端实体在合理的往返时延（RTT）内未收到确认，那么对应的数据包就被假设为已丢失并进行重传。TCP 用一个校验和函数来检验数据是否有错误，在发送和接收时都要计算校验和。[iii]

4. HTTP 协议：

超文本传输协议（英语：HyperText Transfer Protocol，缩写：HTTP）是一种用于分布式、协作式和超媒体信息系统的应用层协议。HTTP 是万维网的数据通信的基础。
HTTP 是一个客户端（用户）和服务端（网站）之间请求和应答的标准，通常使用 TCP 协议。通常，由 HTTP 客户端发起一个请求，创建一个到服务器指定端口（默认是 80 端口）的 TCP 连接。HTTP 服务器则在那个端口监听客户端的请求。一旦收到请求，服务器会向客户端返回一个状态，比如"HTTP/1.1 200 OK"，以及返回的内容，如请求的文件、错误消息、或者其它信息。[iv]

5. h1 下载国科大页面的过程：

(1) Wget 命令会将域名 www.ucas.ac.cn 通过 DNS 协议解析为相应的目的服务器 IP 地址；

(2) 解析获取到目的服务器的 IP 地址后，wget 会选择一个大于 1024 的本机端口向目标 IP 地址的 80 端口发起 TCP 连接请求，与目的主机握手成功后，连接建立完成；
(3) Wget 通过向目的服务器 IP 发出 GET 方法报文（HTTP 请求），该 GET 报文通过 TCP > IP(DNS) > MAC(ARP) > 网关 > 目的服务器；
(4) 目的服务器收到数据帧，通过 IP > TCP > HTTP，目的主机通过 HTTP 协议从请求信息中获得我的主机想要访问的主机名，想要访问的 web 应用和资源，并按照 HTTP 协议格式将 web 资源封装为 HTML 形式的数据(HTTP 响应)；
(5) 该 HTML 数据通过 TCP > IP > MAC >网关 > 我的主机，我的主机收到数据帧，下载完毕；[v]

八、 参考文献

[i] https://zh.wikipedia.org/wiki/%E5%9C%B0%E5%9D%80%E8%A7%A3%E6%9E%90%E5%8D%8F%E8%AE%AE

[ii] https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D%E7%B3%BB%E7%BB%9F

[iii] https://zh.wikipedia.org/wiki/%E4%BC%A0%E8%BE%93%E6%8E%A7%E5%88%B6%E5%8D%8F%E8%AE%AE

[iv] https://zh.wikipedia.org/wiki/%E8%B6%85%E6%96%87%E6%9C%AC%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE

[v] https://blog.csdn.net/u012862311/article/details/78753232?depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-1&utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-1