SDN实验报告

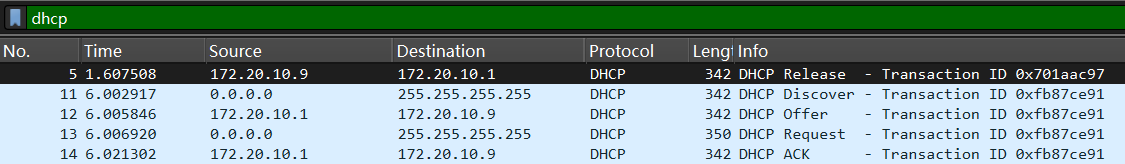
一、DHCP协议

DHCP全称是Dynamic Host configuration protocol，中文名为动态主机配置协议。是一种帮助计算机从指定的DHCP服务器获取它们的配置信息的自举协议。

DHCP使用客户端/服务器模式，请求配置信息的计算机叫做DHCP客户端，提供信息的叫做DHCP的服务器。DHCP为客户端分配地址的方法有三种：手工配置、自动配置、动态配置。主机地址动态分配任务由网络主机驱动。当DHCP服务器接收到来自网络主机申请地址的信息时，才会向网络主机发送相关的地址配置等信息，以实现网络主机地址信息的动态配置。

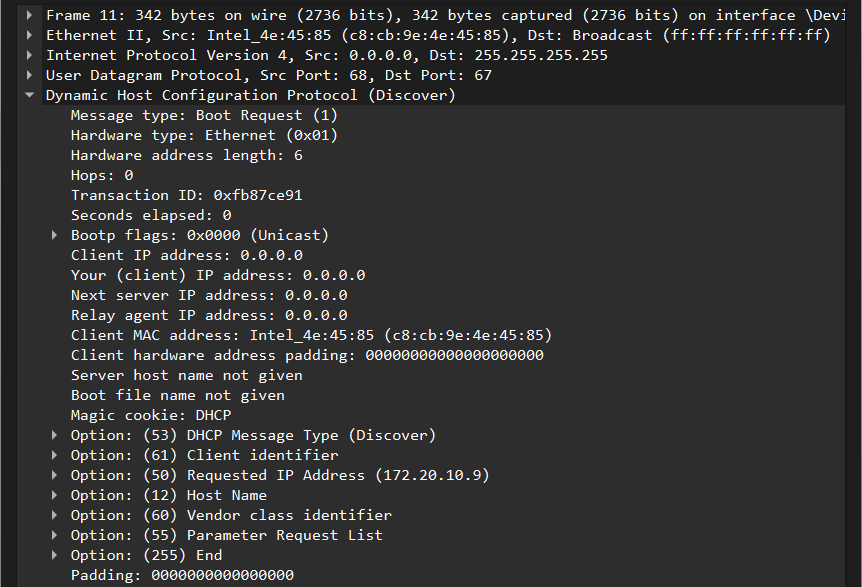
在Windows下通过cmd输入ipconfig /release及ipconfig /renew命令

重新配置IP地址等参数。

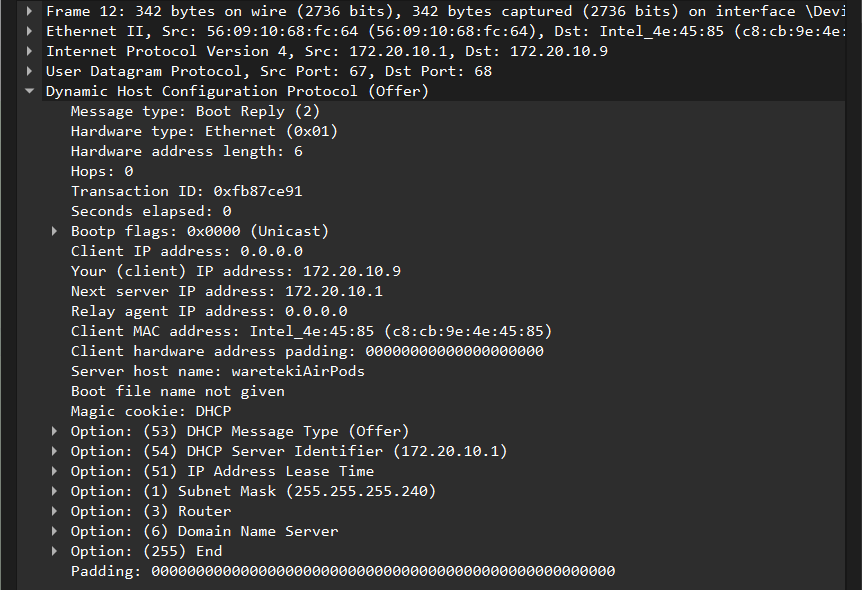


1. DHCP Discover

DHCP客户端在请求IP地址时并不知道DHCP服务器的位置，因此DHCP客户端会在本地网络内以广播方式（广播地址：255.255.255.255）发送Discover请求报文，以发现网络中的DHCP服务器。所有收到Discover报文的DHCP服务器都会发送应答报文，DHCP客户端据此可以获取DHCP服务器的位置。客户端此时还不知道自己属于哪一个网路﹐所以数据包的源IP地址为0.0.0.0。

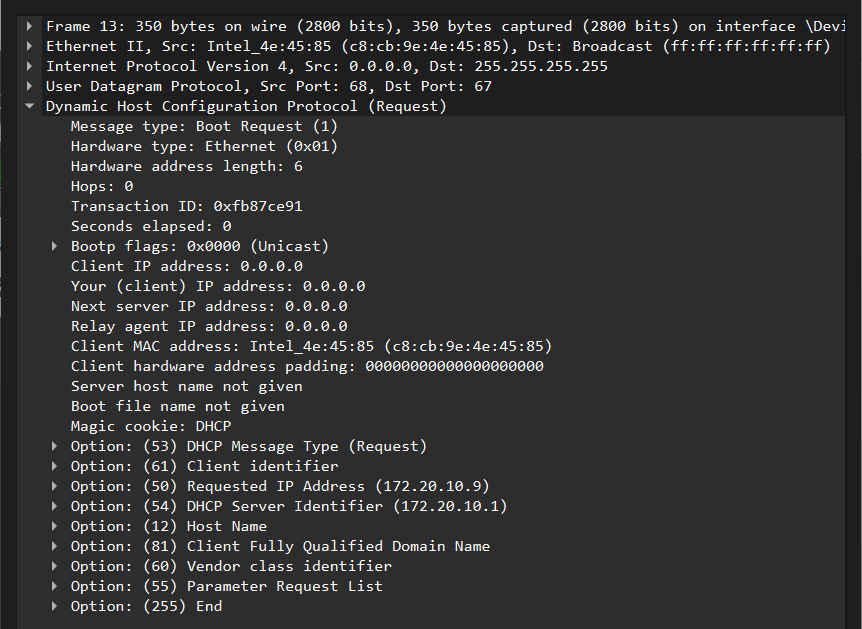
2. DHCP Offer

DHCP服务器收到Discover报文后，就会在所配置的地址池中查找一个合适的IP地址，加上相应的租约期限和其他配置信息（如网关、DNS服务器等），构造一个Offer报文，发送给DHCP客户端，告知用户本服务器可以为其提供IP地址。



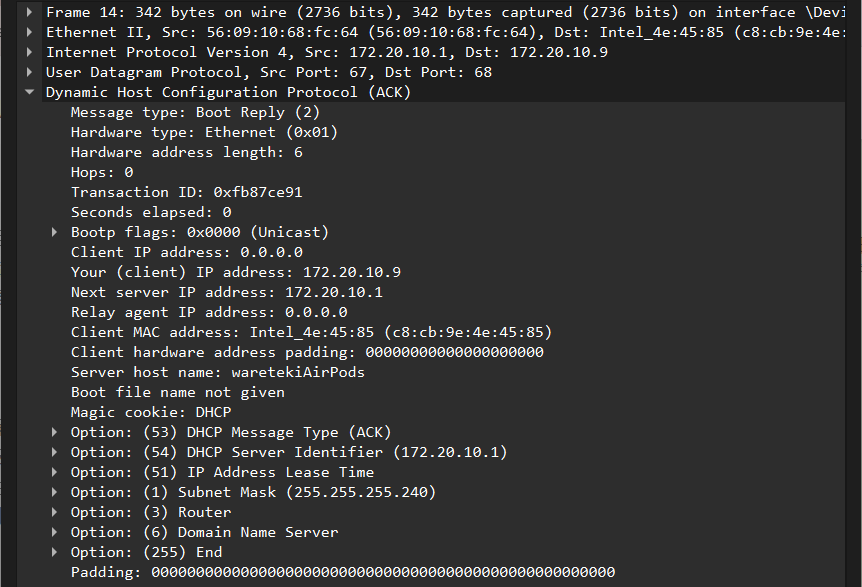
3. DHCP Request

DHCP客户端可能会收到很多Offer请求报文，所以必须在这些应答中选择一个。通常是选择第一个Offer应答报文的服务器作为自己的目标服务器，并向该服务器发送一个广播的Request请求报文，通告选择的服务器，希望获得所分配的IP地址。



1. DHCP ACK

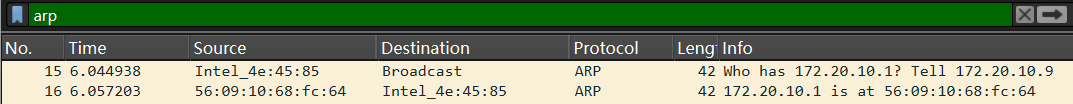
DHCP服务器收到Request请求报文后，根据Request报文中携带的用户MAC来查找有没有相应的租约记录，如果有则发送ACK应答报文，通知用户可以使用分配的IP地址。



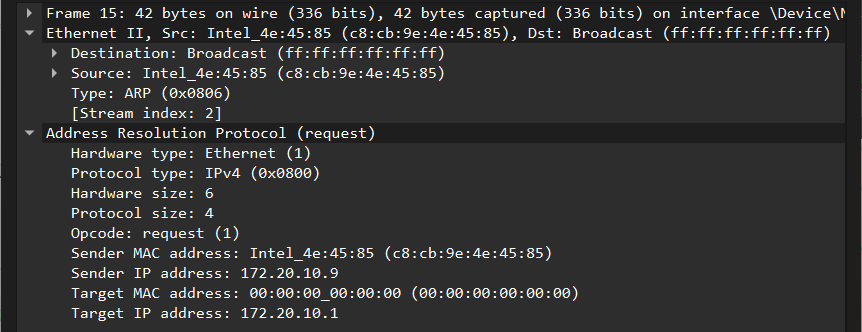
1. ARP协议

ARP全称是Address Resolution Protocal，中文名是地址解析协议。是将IP地址解析为以太网的MAC地址的协议。

在局域网中，当主机或其他网络设备有数据要发送给另一个主机或设备时，它必须知道对方的IP地址。但是因为IP数据报文必须封装成帧才能通过物理网络发送，发送站还必须有接收站的物理地址，所以需要一个从IP地址到物理地址的映射。ARP就是实现这个功能的协议。

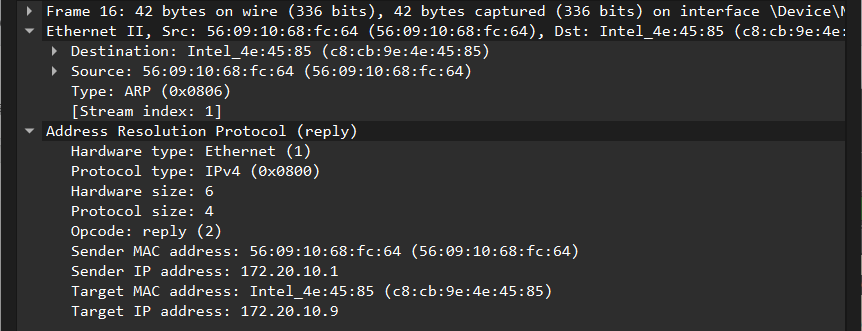


1. ARP请求报文



由于此时主机不知道网关的MAC地址，故主机会将包含网关IP地址的ARP请求广播到局域网络上的所有主机，并接收返回消息，以此确定网关MAC地址。

1. ARP应答报文



网关收到广播的ARP请求报文后，发现报文中携带的IP地址与自己的相同，便将自己的MAC地址填入ARP响应报文，并传送给请求主机。

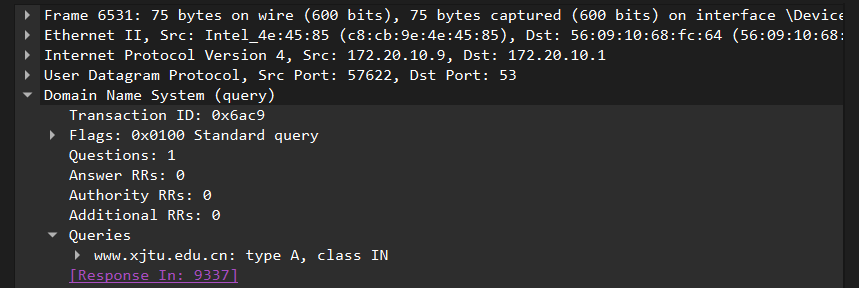
1. DNS协议

DNS，全称是Domain Name System，中文名为域名系统。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，允许终端设备将给定的人类可读URL转换为网络可以理解的机器可用IP地址，能够使人更方便地访问互联网。

1. DNS查询报文



使用UDP协议

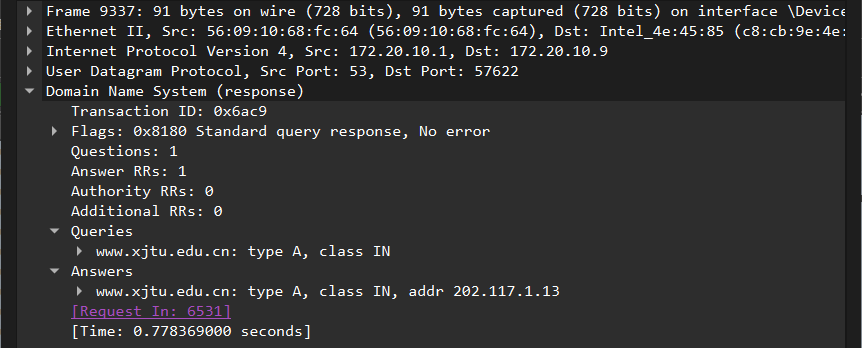
目的地址与本机默认DNS相同（172.20.10.1）

源端口为57622，目的端口为53

域名解析记录为A记录，表示记录了DNS域名对应的IP地址

解析出的IP地址显示为class IN，表示查询的域名为互联网地址

1. DNS回复报文



使用UDP协议

源IP地址与本机默认DNS服务器地址相同（172.20.10.1）

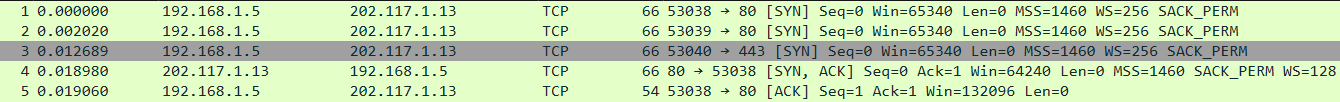
源端口为53，目的端口为57622

域名解析记录为A记录，解析出的IP地址显示为class IN，表示查询的域名为互联网地址，地址为202.117.1.13

四、TCP协议

TCP全称是Transmission Control Protocol，中文名为传输控制协议。是为了在不可靠的 互联网络上提供可靠的端到端字节流而专门设计的一个传输层协议。

1. TCP三次握手建立连接：



（1）第一次握手（报文1）：

客户端向服务器202.117.1.13发起连接请求，向服务器发送SYN置1的报文，序列号Seq=0，来通知服务器客户端的存在，以便服务器知道客户端希望建立连接，客户端进入SYN\_SEND状态。

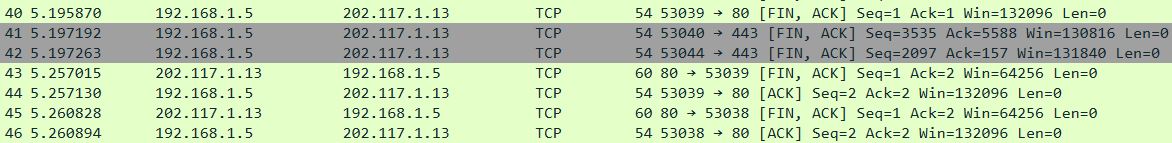
（2）第二次握手（报文4）：

服务器收到SYN报文后应答客户端，发送SYN和ACK都置1的报文，Seq=0，ACK=0+1=1（第一次握手的Seq值+1），来确认服务器已经接收到客户端的连接请求，并告知客户机服务器也愿意建立连接，此时服务器进入SYN\_RECV状态。

（3）第三次握手（报文5）：

客户端收到服务器的SYN+ACK报文后应答服务器，发送一个ACK置1的报文，Seq=1（与第二次握手的Ack值相同），ACK=0+1=1（第二次握手的Seq值+1），确认双方都已知道连接已经建立，并且可以开始进行数据传输，这是连接建立的最后一步，客户端和服务器都进入ESTABLISHED状态，完成三次握手。

1. TCP四次挥手释放建立：



（1）第一次挥手（报文40）：

客户端向服务器发送一个FIN数据包，FIN和ACK都置为了1，Seq=1，

发起数据方主动断开连接，此时主机处于FIN\_WAIT1状态。

（2）第二次挥手（报文43）：

服务器收到FIN数据包之后，向客户端发送确认包，ACK置为1,Seq=1，Ack=1+1=2（第一次挥手的Seq值+1），表明已经接收到了发起方的关闭请求。服务器还有数据没有发送完，等发送完了所有的数据就进行第三次挥手。此时服务端处于CLOSE\_WAIT状态，客户机处于FIN\_WAIT2状态。

（3）第三次挥手（报文45）**：**

服务器向主机发送FIN数据包，FIN和ACK都置为1，Seq=1，Ack=2（与第二次挥手的Ack值相同），这是接收方发起的关闭请求，表示接收方没有更多数据要发送了。此时服务端处于LAST\_ACK状态，客户端处于TIME\_WAIT状态。

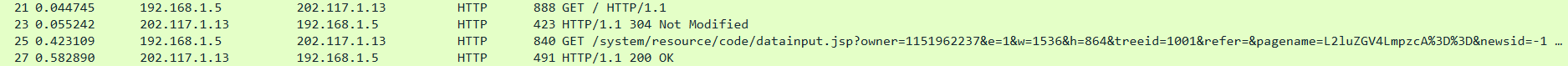
（4）第四次挥手（报文46）**：**

客户机收到FIN数据包之后，发送一个应答报文，ACK置为1，Seq=2，Ack=2（第三次挥手的Seq值+1），发起方接收到了接收方的关闭请求，此时客户端处于TIME\_WAIT状态。

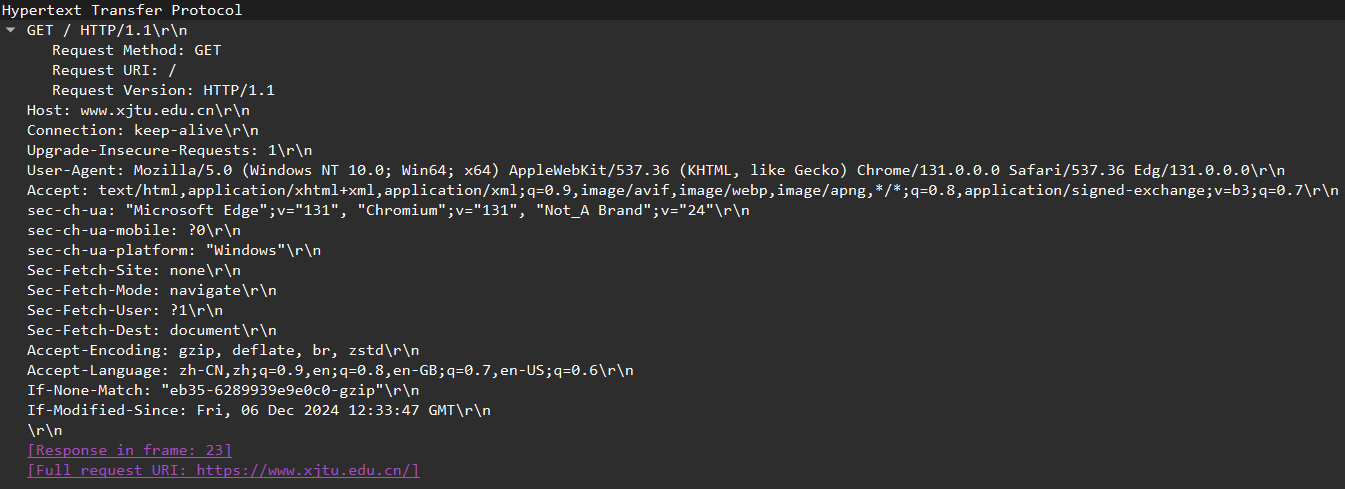
五、HTTP协议

HTTP 全称是HyperText Transfer Protocol，中文名是超文本传输协议。它是基于TCP协议的应用层协议，就是客户端和服务端进行数据传输的一种规则。

HTTP报文分为客户端发往Web服务器的请求报文和Web服务器发往客户端的响应报文两类。这两种类型的消息由一个请求行、一个或者多个头部行、一个表示头部行结束的空行和可选的附属体组成。



1. 请求报文



(1)请求行：GET / HTTP/1.1\r\n

由3部分组成：请求方法、请求目标、协议版本

请求方法：GET

请求的URI路径：/（网站的默认首页）

HTTP版本：1.1

(2)请求头部：

Host：接受请求的服务器域名，www.xjtu.edu.cn

Connection：指定与连接相关的属性，keep-alive，持续连接方式

User-Agent：包含HTTP客户端运行的浏览器类型，

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0

Accept：客户端能接收到的内容类型，内容类型的先后次序表示客户端接收的先后次序。text、application、image

Accept-Encoding：通知服务端可以发送的数据压缩格式，

gzip, deflate, br, zstd

Accept-Language：通知服务端可以发送的语言，

zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

(3)请求正文：

可选部分，包含请求的数据，GET请求没有请求正文

1. 应答报文



(1)状态行：

由3部分组成：HTTP版本、状态码、相应的状态信息

HTTP版本：1.1

状态码：200，属于处理成功相应类

状态消息：OK，请求已成功，服务器返回了请求的资源

(2)响应头部：

Server：服务器应用程序软件的名称和版本，China Webber /1.1

Pragma：包含实现特定的指令，no-cache，响应消息不能缓存

Content-Type：响应正文的类型，image/gif;charset=UTF-8

Content-Length：响应正文长度，0

Set-Cookies：由服务器生成，发送给客户端，客户端浏览器会将Cookies

的值保存

Connection：指定与连接相关的属性，keep-alive，持续连接方式

Content-Language：响应正文使用的语言，zh-CN

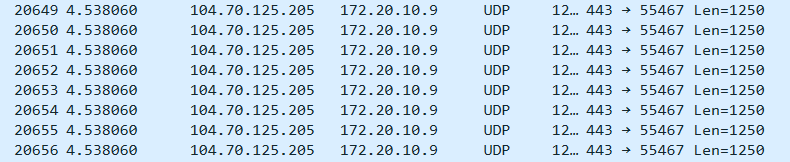
(3)消息体：

包含响应的数据，例如HTML页面内容

1. UDP协议

UDP全称是User Datagram Protocol，中文名为用户数据报协议。是一个简单的面向消息 的传输层协议，尽管UDP提供标头和有效负载的完整性验证，但

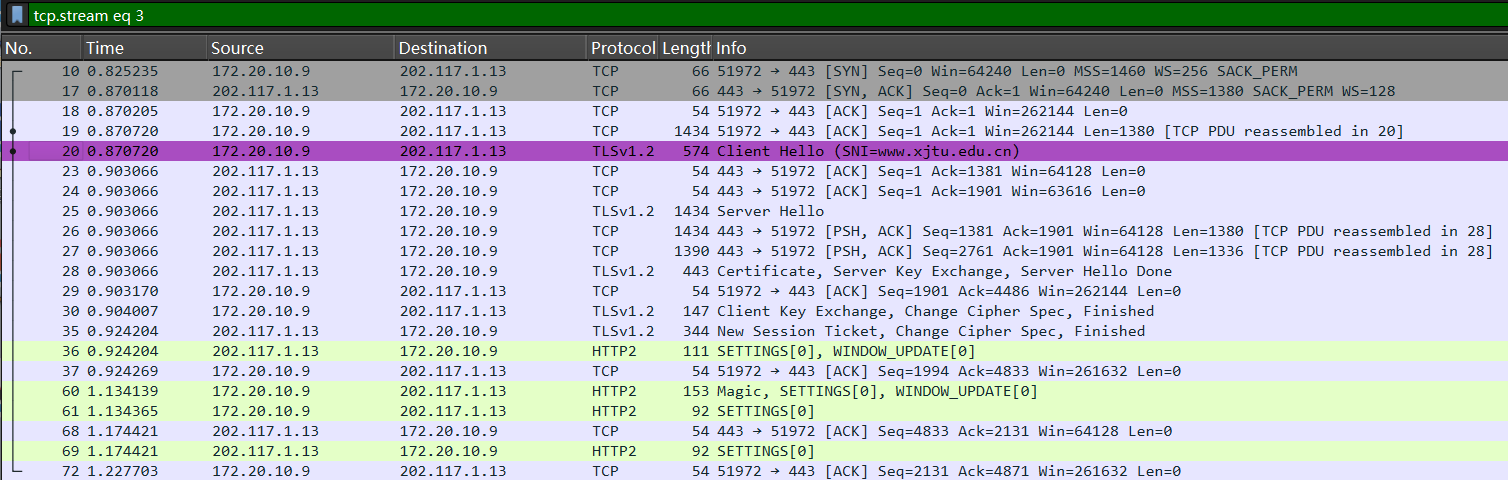
它不保证向上层协议提供消息传递，并且在发送后不会保留UDP消息的状态。因 此，UDP有时被称为不可靠的数据报协议。如果需要传输可靠性，则必须在用户 应用程序中实现。



1. TLS协议

全称是Transport Layer Security，中文名为安全传输层协议。用于在两个通

信应用程序之间提供保密性和数据完整性。



TLS加密传输的建立过程

1. 客户端发起握手

客户端向服务器发起TLS握手请求Client Hello，并发送支持的TLS版本、加密套件列表、随机数等信息。

SNI表示客户端想要访问的服务器域名是www.xjtu.edu.cn。SNI用于在同一个IP地址上托管多个域名时，帮助服务器选择正确的证书。

1. 服务器响应

服务器响应客户端的Client Hello，发送Server Hello消息，服务器选择TLSv1.2作为通信协议，并确定了加密套件，并且生成一个随机数，用于后续的密钥交换。

1. 服务器发送证书和密钥交换信息

Certificate证书中包含了服务器的公钥和域名信息。

Server Key Exchange是服务器发送的密钥交换信息，用于后续的密钥协商。

Server Hello Done表示服务器已经完成了握手的第一阶段，等待客户端响应。

1. 客户端密钥交换和加密切换

Client Key Exchange表示客户端生成一个预主密钥，并使用服务器的公钥加密后发送给服务器。

Change Cipher Spec表示客户端将切换到加密通信模式。

Finished消息是客户端发送的第一个加密消息，用于验证握手过程的完整性。

1. 服务器完成握手

New Session Ticket用于支持会话恢复，以便在未来的连接中减少握手时间。

Change Cipher Spec表示服务器也将切换到加密通信模式。

Finished消息是服务器发送的第一个加密消息，用于验证握手过程的完整性。