|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验4 | **实验名称** | IPv4 |
| **姓名** | 李彦浩 | **学号** | 202100300063 |
| **班级** | 工业软件班 | **成绩** | （空着） |
| 1. **实验目的**   了解互联网协议(IP)的详情。IP是整个网络层所使用的协议。本次实验将研究IPv4，因为它是普遍部署的，而IPv6是部分部署的 | | | |
| 1. **实验要求**   wireshark：使用wireshark软件工具用于捕获和检查数据包跟踪。。  wget：使用wget(windows下)来抓取web资源。  traceroute：确定网络数据包在到达目标主机的过程中经过的路由。 | | | |
| 1. **实验内容**   例子：   1. Capture a Trace. 2. Inspect the Trace 3. IP Packet Strucutre 4. Internet Paths 5. IP Header Checksum 6. Explore on your own | | | |
| 1. **实验过程**  Step 1:Capture a Trace(链路追踪) 首先确保计算机有IPv4连接。  选择一个远程服务器得URL，比如本校的：[https://www.sdu.edu.cn/。然后wget:](https://www.sdu.edu.cn/%E3%80%82%E7%84%B6%E5%90%8Ewget:)  wget -P C:\Users\Administrator\Desktop\junior1\computer\_network\exp\target <http://www.sdu.edu.cn/>  1  然后对之前选择的远程主机traceroute  tracert [www.sdu.edu.cn](http://www.sdu.edu.cn)  2  每一行展示了从发起traceroute的主机到目标主机之间的下个IP节点跳跃。如果出现“\*”这个符号，代表网络没有响应来识别该Internet路径段。  开启Wireshark，过滤器：  tcp port 80  确保域名解析也开了。  用wireshark抓wget的包。  3 Step 2:Inspect the Trace(追踪分析) 随便调一帧，主要看其中的IP帧头。  4   1. Version字段：标识IP版本，这里是IPv4 2. Header Length字段：帧头长度 3. Differentiated Services字段：标识数据帧服务质量与路由中流量拥堵的迹象 4. Total Length字段：整帧长度 5. Idetification字段：用来组装碎片。当一个大的IP包被拆成很多小的帧发送时，会产生很多碎片(fragment)。这个字段后面紧跟的就是Flags&Fragment Offset字段，也和碎片相关。 6. Time to Live字段：超时时间 7. Protocol字段：多路分解键，标识更高一层的协议。 8. Header Checksum字段：帧头校验和。 9. Source & Destination字段：源主机与目标主机IP地址 10. 剩下的部分就是IP协议的负载了，比如TCP协议帧头  Step 3:IP Packet Structure(IP帧结构) 画出IP帧结构图。   |  |  |  |  | | --- | --- | --- | --- | | Version 4bit | Header Length 4bit | Differentiated Services 1B | Total Length 2B |  |  |  |  |  |  | | --- | --- | --- | --- | --- | | Identification 2B | Flags 3bit | Fragment Offset 13bit | TTL 1B | Protocol 1B |  |  |  |  | | --- | --- | --- | | Header CheckSum 2B | Source 4B | Destination 4B |   Q1:你的计算机和远程主机的IP地址是什么？  5  我的计算机：10.27.243.63  远程主机：202.194.7.118  Q2:Total Length字段指的是IP帧头加IP负载，还是仅仅IP帧头？  6  IP帧头20字节。  7  IP负载（TCP层）32字节。  Total Length 52字节。  所以TL字段指的是IP帧头加IP负载。 Q3:Identification字段是在变化的还是每个帧都一样？如果发生变化，有什么规律？ 每个帧不一样。在同一传输方向上，Identification是连续递增1的。比如371，372帧  8  9  他俩都是从202.194.7.118发到10.27.243.63上的。可以看到一个id23206，一个23207。连续增1。  但如果不是同一传输方向上的，比如367和368，那就不一样了。因为这个标识字段来自不同主机的IP软件，而不同端的标识初始值也不一样，所以很可能不是连续递增1的。  10  11  这个字段的意义是：IP软件维护一个计数器，每有一帧产生（可能是分片的帧），就在计数器里+1，然后把计数器的值赋给这个字段，以此标识帧。 Q4:TTL的初始值是多少？这个值已经达到可能的最大值了吗？ 我抓到的初始值是128。为了防止数据包一直在网络中传输，就赋予它一个时间片，每经过一个路由器，剩余时间-1。直到超时不再转发为止。  一般在IPv4里最大初始值是64，但是在我电脑上是128。 Q5:如何查看一个包是否被分片了？ 在Flags字段中，可以看到三个bit位，其中后两个表明了是否分片，第二个bit为1表示未分片。否则分片。  12 Q6:IP帧头的长度是多少？是如何被编码进Header Length字段的？提示：这个字段只有4bit，而version字段占了4个字节 由于整个帧头的长度是固定的（20B）。而version字段也是确定的（总归得知道是哪个版本的IP协议），因此我们可以用20去除以version字段的值，比如你是IPv4，那么就得到20/4=5。然后把5存到Header Length字段里。 Step 4:Internet Paths(网络路径) IP协议中的Source/Destination仅表示源和目标节点两个终端的IP地址，并不涉及中间路由。traceroute的工作原理是：每到一个中间路由，就向源节点发一个响应。这样源节点就知道它途径了什么中间节点。  画出traceroute的网络路径图。并附上traceroute的结果。  13  14 Step 5:IP Header Checksum(IP帧头校验和) 从抓到的数据包中选取一个从远程服务器到本地计算机的帧，且帧头校验和不为0。  15  用校验和计算校验结果的流程：   1. 将20个字节分成10个2字节 2. 将10个2字节加起来 3. 如果结果多余4位，把多余部分拆出来，然后加回剩余部分，例如：   5a432->a432+5->a437   1. 最终结果应该是0xffff，或者说，-0（因为是补码形式）   比如在我这里10个2B分别为：   | **45 00** | **00 34** | **c0 d7** | **40 00** | **31 06** | **0d 4e** | **b6 3d** | **c8 06** | **0a 1b** | **f3 3f** | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |   加起来得到：  3FFFC  把3拿出来，加到FFFC里得到  0XFFFF。正确。  开启wireshark的校验选项。Preferences→Protocols→IPv4→Validate IPv4 checksum as possible  16  wireshark也给出correct的结果。 Explore on your ownQ1:读一读并尝试实验一下IPv6。大多数现代操作系统都支持IPv6。然后抓一下IPv6的包。捕获IPv6 我的电脑已经支持了IPv6。查看方式：  # Windows 10  控制面板->网络和Internet->网络和共享中心->更改适配器设置->WLAN->(右键)属性->勾选Internet协议版本6  17  过滤器:  ip.version==6  捕获到IPv6，可以看到协议字段和IPv4有很多不一样的地方。  18 和IPv4的异同 IPv6和IPv4不同的地方在于：   1. IPv4地址用”.”分隔，而IPv6以”:”分隔 2. IPv4有4个8位，而IPv6有8个16位   很多时候IPv6实在太长了，因此可以省略一部分0X0000。例如：  1111::2222  如果作为一个IPv6地址，那么意味着中间省略了6组0000（总共8组）  但”::”只能有1个。 寻址过程 IPv6在寻址时有以下三个段。  19  先通过站点前缀找到站点，然后追踪子网，再找到接口 Q2:学习隧道(tunnels)，他将一个IP包包裹在另一个IP帧头中。tunnels是如何产生的？ 为了解决这个问题：  两个IPv6网络需要进行通信，途径一个IPv4网络。  20  在两个IPv6的网络出口网关处，实现一段地址转换程序。  tunnel就是将IPv6的流量封包到了IPv4的数据包中，然后通过IPv4网络传输。 Q3:尝试一下IP geolocation(IP定位)，他是通过Name Administrative Databases(命名管理数据库)。试一试Geolocation Service。 百度就提供了IP反查地理位置的服务，随便输一个看看。  21  具体实现原理之后进行学习。 Q4:了解以下IPsec或IP security。它为IP数据包提供了可信任凭证，并经常被用来作为VPN(virtual private network)的组成部分。 IPSec（IP Security）是一种三层隧道加密协议，它为IP数据报提供了高质量的、可互操作的、基于密码学的安全性。IPSec在IP层通过加密与数据源认证等方式，提供了以下的安全服务：   1. 数据机密性（Confidentiality）：IPsec发送方在通过网络传输包前对包进行加密。 2. 数据完整性（Data Integrity）：IPsec接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改。 3. 防重放（Anti-Replay）：IPsec接收方可检测并拒绝接收过时或重复的报文。 | | | |
| **四．实验心得**  本次实验我在实验指导书的指引下，探究了IP协议及其各个字段的用途与含义。比如IPv4的版本号、IPv4帧头长度以及IPv4 Header Length之间的关系。此外，我还学习到了如何采用1s completion checksum来计算校验结果的方式。  不仅是IPv4，我还通过Explore on your own部分探究了IPv6协议。以及tunnel技术。tunnel技术在两个IPv6的网络出口网关处，实现一段地址转换程序。本质上将IPv6的流量封包到了IPv4的数据包中，然后通过IPv4网络传输。  本次实验为我之后进一步学习计算机网络打下了非常重要的基础。 | | | |