计算机学院 计算机网络 课程实验报告

|  |  |  |
| --- | --- | --- |
| 实验题目：IP | | 学号：202200400053 |
| 日期：2024-05-17 | 班级： 2班 | 姓名： 王宇涵 |
| Email：1941497679@qq.com | | |
| 实验方法介绍：  使用traceroute进行抓包, 通过wireShark分析数据包来理解IP协议的组成部分, 包括基础IPv4协议, 片段化, IPv6三个部分. | | |
| 实验过程描述：    **1. 选择通过 traceroute 命令发送到 gaia.cs.umass.edu 的计算机发送的第一个 UDP 段（提示：这是 ipwireshark-trace1-1.pcapng 文件中的跟踪文件中的第 44 个数据包）。展开数据包详细信息窗口中的 Internet 协议部分。你的计算机的 IP 地址是什么？**    答 : 192.168.86.61  **2. IPv4 数据报头中 TTL 字段的值是多少？**    答 : 1  **3. IPv4 数据报头中的上层协议字段的值是多少？**    答 : 为UDP(17)  **4. IP 头中有多少字节？**    答 : 20bytes  **5. IP 数据报的有效载荷中有多少字节？解释一下你是如何确定有效载荷字节数的。**    答 : 36bytes : 56 – 20 = 36bytes  **6. 这个 IP 数据报是否被分片？解释一下你是如何确定数据报是否已被分片的。**    答 : 没有被分片, 可以看出Not Set    **7. 在由你的计算机发送到 128.119.245.12 的 traceroute 路由器序列中，IP 数据报中的哪些字段会随着每个数据报的发送而不断变化？为什么会变化？**        答 : 标识位 , 校验和, 生命周期一直在变化, 因为目的地端口一直在改变, 网络路由器对数据报进行处理时所做的更改引起.  **8. 在这个包含 UDP 段的 IP 数据报序列中，哪些字段保持不变？为什么会保持不变？**              答 : 总长, 版本号, 头文件长度, 服务类型, 标志位, 分片偏移量, 上层协议类型, 源地址和目的地址均保持不变因为这些数据报具有相同的 IP 头部信息，它们在网络中的路由和处理方式也应该是相同的.  **9. 描述一下你在你的计算机发送的 IP 数据报的标识字段中看到的值的模式。**        答 : 发现是连续且每次加1的.    **10. 从路由器返回的 IP 数据报中指定的上层协议是什么？[注意：对于 Linux/MacOS，答案与 Windows 不同]。**    答 : ICMP  **11. ICMP 数据包序列中的标识字段的值（跨所有路由器的所有 ICMP 数据包）在行为上是否类似于您上面对问题 9 的回答？**      答 : 不类似, 对于不同路由器发送的数据包, 无法做到连续性, 对于相同路由器且数据包编号相差1的仍然能做到连续性.  **12. 在所有路由器的所有 ICMP 数据包中，TTL 字段的值是否相似？**  答 : 不同路由器的TTL不同, 相同路由器的TTL相同.    **13. 找到由你的计算机通过 traceroute 命令发送到 gaia.cs.umass.edu 的第一个 UDP 段的第一个部分所在的第一个 IP 数据报，之后你指定 traceroute 数据包长度为 3000。（提示：这是位于脚注2中的 ip-wireshark-trace1-1.pcapng 跟踪文件中的第179个数据包。数据包179、180和181是对第一个发送到 128.119.145.12 的 3000 字节 UDP 段进行分片得到的三个 IP 数据报）。该段是否已被分片成多个 IP 数据报？（提示：答案是 yes）**    答 : yes  **14. IP 头部中的哪些信息表明该数据报已被分片？**    答 : more fragments : set.  **15. IP 头部中的哪些信息表明这是第一个片段还是后续片段？**      答 : Fragment Offset为0代表是第一个片段, 否则为后续片段  **16. 这个 IP 数据报中有多少字节（头部加有效载荷）？**    答 : 1500字节  **17. 现在检查包含分片 UDP 段的第二个片段的数据报。IP 头部中的哪些信息表明这不是第一个数据报片段？**    答 : 此时有偏移量代表不是第一个数据包片段.  **18. 在第一个和第二个片段之间 IP 头部中有哪些字段发生变化？**      答 : 片段偏移量和校验和  **19. 现在找到原始 UDP 段的第三个分片所在的 IP 数据报。IP 头部中的哪些信息表明这是该段的最后一个片段？**    答 : More Fragments : Not set表示是最后一个片段    **20. 进行 DNS AAAA 请求的计算机的 IPv6 地址是什么？这是跟踪中的第 20 个数据包。给出该数据报的 IPv6 源地址，其格式与 Wireshark 窗口中显示的完全相同。**    答 : 2601:193:8302:4620:215c:f5ae:8b40:a27a  **21. 该数据报的 IPv6 目的地址是什么？以与 Wireshark 窗口中显示的完全相同的形式给出该 IPv6 地址。**    答 : 2001:558:feed::1  **22. 该数据报的流标签（Flow Label）的值是多少？**    答 : 0x63ed0  **23. 此数据报中携带了多少有效载荷数据？**    答 : 37bytes  **24. 此数据报的有效载荷将在目的地被交付给哪个上层协议？**    答 : UDP    **25. 对于此 AAAA 请求，DNS 响应中返回了多少个 IPv6 地址？**    答 : 返回了1个IPv6地址  **26. 对于 youtube.com 的 DNS 返回的第一个 IPv6 地址是什么（在 ip-wireshark-trace2-1.pcapng 跟踪文件中，这也是数字上最小的地址）？以与 Wireshark 窗口中显示的完全相同的简写形式给出此 IPv6 地址。**    答 : 172.217.10.142 | | |
| 分析：  IPv4（Internet Protocol version 4）是互联网上广泛使用的第四版 Internet 协议。它定义了互联网上每个设备的唯一标识符，称为 IP 地址。IPv4 地址由 32 位二进制数字组成，通常被分成四个八位的数字，以点分十进制表示，如 192.0.2.1。  片段化是指在网络传输过程中，将原始数据包分割成更小的片段以适应网络链路的最大传输单元（MTU）。这种分割通常发生在发送端的路由器上，而在接收端的路由器上再次组装。片段化允许大的数据包在不同网络中传输，因为不同网络链路可能有不同的最大传输单元。  IPv6（Internet Protocol version 6）是 IPv4 的继任者，设计用来解决 IPv4 地址空间有限的问题。IPv6 使用了 128 位的地址空间，相比 IPv4 的 32 位，地址数量大大增加，几乎可以满足任何未来的互联网需求。 | | |
| 结论：  在本次实验中，我学到了如何使用 Wireshark 工具和traceroute来抓取分析网络数据包。  通过分析网络数据包，我能够了解到在网络通信过程中发生的各种事件和细节，包括数据报的分片、IP 地址的解析、上层协议的使用等。  我还学会了查看和理解 IP 头部中的各个字段，以及如何根据这些字段的值来判断数据报的特性，比如是否分片、是否是第一个分片等。  此外，我还学会了如何解析 DNS 请求和响应，以及如何查找特定的网络活动，如 DNS 查询和 ICMP 响应。  通过这些分析，我对网络通信的工作原理有了更深入的理解，也提升了我的网络分析技能。 | | |