|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验4 | **实验名称** | IPv4 |
| **姓名** | 杨伟康 | **学号** | 202200201095 |
| **班级** | 网安班 | **成绩** | （空着） |
| 1. **实验目的**   要了解IP（互联网协议）的详细情况。IP是互联网中使用的网络层协议。我们将探讨IPv4版本，因为它已被广泛部署，而IPv6版本则部分部署。IP的内容涵盖在你的文本的5.6.1节至5.6.3节。在做这个实验室之前，请先复习这些部分。。 | | | |
| 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/curl：这个实验室使用wget（Linux和Windows）和curl（Mac）来获取web资源。wget和curl是命令行程序，可以获取URL并执行整个页面，wget和curl让您可以准确地控制您获取的URL  traceroute/tracert：这个实验室使用“traceroute”来找到从您的计算机和远程互联网主机。traceroute是用于发现Internet路径的标准命令行实用程序您的计算机使用的 | | | |
| 1. **实验内容** 2. Capture a Trace. 3. Inspect the Trace 4. IP Packet Structure 5. Internet Paths 6. IP Header Checksum | | | |
| 1. **实验过程**   Step 1: Capture a Trace.  使用提供的跟踪，获得了如下的数据，你现在应该有一个类似于下图所示的短跟踪，以及traceroute的输出较早运行到相应的服务器。    Step 2: Inspect the Trace  在追踪中选择任意数据包，并展开IP头部字段（使用“+”展开器或图标）以查看详细信息。你可以简单地在顶部面板中点击一个数据包来选择它。你将在中部面板看到该数据包结构的详细信息，并在底部面板看到组成该数据包的字节。我们关注的是IP头部，你可以忽略其他高层和低层协议。当你点击IP头部的部分时，你会在底部面板看到与高亮部分相对应的字节。我们在上面的图中已经展开了IP头部，并点击了所有的IP头部字段。  版本字段设置为4，这毕竟是“IPv4”    接下来是头部长度字段。通过观察数据包数据中选择的字节，可以看到版本和头部长度都打包在一个字节中。    差分服务字段包含位标志，用于指示数据包是否应在路由器上根据服务质量和拥塞指示进行处理。    然后是总长度字段。    接下来是标识字段，当大的IP数据包被发送为多个称为片段的较小部分时，该字段用于对片段进行分组。它后面是标志和片段偏移字段，它们也与片段化相关。注意，它们共享字节。    然后是生存时间（TTL）字段，后面是协议字段。    接下来是头部校验和。是否你的头部校验和显示为0，并且被标记为从你电脑发送到远程服务器的IP数据包校验和    头部中的最后两个字段通常是源地址和目的地址。IP数据包中可能存在IP选项，但在标准的Web流量中这些选项不太可能出现。    IP头部后面是IP有效载荷。这构成了数据包的其余部分，从下一个更高层的头部开始，在我们的情况下是TCP，但不包括任何链路层尾部（例如，以太网填充）。    Step 3: IP Packet Structure  为了展示你对IP的理解，请画出你研究过的IP数据包的示意图。    **你电脑的IP地址和远程服务器的IP地址分别是什么？**    **“总长度”字段是否包括IP头部加上IP有效载荷，还是只包括IP有效载荷？**  “总长度”字段在IP头部中确实包括IP头部加上IP有效载荷的长度。  **对于不同的数据包，识别（Identification）字段的值是如何变化或保持不变的？例如，在一个TCP连接中的所有数据包是否都保持相同的值，还是每个数据包都不同？两个方向上的值是否相同？如果值发生了变化，你能看出任何模式吗？**  识别（Identification）字段的值对于不同的数据包通常是不同的，以唯一标识每个IP数据报。在一个TCP连接中，每个数据包的识别（Identification）字段值也可能是不同的，特别是当数据包需要被分片时。两个方向上的值通常是不同的，而值的变化模式可能取决于发送方在生成IP数据报时采用的策略。  **从你的电脑发送的数据包的TTL字段的初始值是多少？它是可能的最大值，还是某个较低的值？**  初始值是128，使用较低的初始TTL值可以帮助在网络中更快地检测和丢弃由于路由循环或其他问题而无法到达目的地的数据包。当TTL值减少到0时，数据包将被丢弃，并发送ICMP报文通知源主机。  **从查看数据包来看，你如何判断它没有被分片？**在正常情况下，IP数据包大多数情况下都不会被分片。但接收方必须有办法确定这一点。  **IP头部的长度是多少，并且这个长度是如何在头部长度字段中编码的？**  IP头部的长度可以是20到60字节之间的任意值，具体取决于数据包是否包含可选字段以及可选字段的长度。  头部长度字段以4字节为单位，通过4位的二进制数来编码头部的长度。最大可表示的长度为60字节。  Step 4: Internet Paths  IP数据包中的源IP地址和目的IP地址表示的是Internet路径的端点，而不是数据包从源地址到目的地址传输过程中经过的网络路径上的IP路由器。traceroute是一种用于发现这条路径的工具。它的工作原理是引发路由器响应（ICMP TTL超过消息），首先从离源地址一跳远的路由器开始，然后是离源地址两跳远的路由器，然后是三跳，依此类推，直到到达目的地址。这些响应将标识路由器的IP地址。traceroute的输出通常会逐行打印关于每个“跳”的信息，包括测量的往返时间（RTT）和路由器的IP地址及DNS名称。DNS名称对于确定路由器所属的组织很有用。由于traceroute利用了常见的路由器实现，因此无法保证它会对路径上的所有路由器都有效，当它在路径的某些部分失败时，通常会看到“\*”作为响应。  在这里插入图片描述  使用traceroute的输出结果，绘制一张网络路径的图示。如果你正在使用提供的trace，请注意我们已经将相应的traceroute输出作为单独的文件提供。  Step 5: IP Header Checksum  现在我们将通过验证数据包来查看IP头部校验和的计算。校验和算法会一次添加16位的头部字节。它的计算方式是，对整个IP头部（包括校验和值）重新计算总和，结果应该为零。对我们来说，一个复杂的因素是，这是使用1的补码算术来进行的，而不是通常用于计算的2的补码算术。下面的步骤解释了如何进行必要的计算。  从trace中，选择一个从远程服务器发送到你的计算机的数据包，并检查校验和字段是否有一个非零值。在网络上发送的校验和值将是非零的，所以如果你有一个零值，那可能是因为捕获设置的原因。为了简化这个练习，尝试一个IP头部为20字节的数据包，这是在没有选项时的最小头部大小。  按照以下步骤来检查校验和值是否正确：   1. 将头部拆分为10个两字节（16位）的字。每个字在Wireshark窗口底部的数据包数据面板中显示为4个十六进制数字，例如，05 8c。 2. 使用常规加法将这10个字相加。你可以使用十六进制计算器（在Google上搜索一个），或者将它们转换为十进制进行相加，然后再转换回十六进制。选择对你来说最方便的方法。 3. 为了从你目前的加法结果中计算出1的补码和，将任何超出（字大小的4位数字）的进位位加回到余数上。例如：5a432 将变为 a432 + 5 = a437。 4. 最终结果应该是 0xffff。这在1的补码形式中实际上是零，或者更准确地说，0xffff 是 -0（负零），而 0x0000 是 +0（正零）。   Explore on your own (IEEE 802.3)  **我们鼓励你在完成这个实验室后自己探索IP。以下是一些建议：**  **• 阅读并尝试使用IPv6。现代操作系统已经支持IPv6，因此你可能能够在你的网络上捕获IPv6流量。你还可以通过隧道连接到IPv6提供商来“加入IPv6”主干网。** | | | |
| **四．实验心得**  在深入学习和实验IPv4（Internet Protocol version 4）的过程中，我获得了许多宝贵的经验和见解。IPv4作为互联网的基础网络层协议，其普及性和重要性不言而喻。以下是我对这次实验探索IPv4的一些心得。我通过实际操作和观察，深入了解了IPv4数据包的格式和传输过程。IPv4数据包由头部和数据部分组成，头部包含了源地址、目的地址、生存时间（TTL）等重要信息。在传输过程中，数据包会经过多个路由器进行转发，每个路由器都会根据数据包头部的信息进行路由选择。这种基于IP地址的路由选择机制，使得数据包能够准确地从源地址传输到目的地址。  我还学习了IPv4的一些重要特性，如分片、校验和等。分片是指当数据包的大小超过网络的最大传输单元（MTU）时，需要将数据包拆分成多个较小的片段进行传输。校验和则是用于检测数据包在传输过程中是否发生错误的一种机制。这些特性保证了IPv4数据包在网络中的可靠传输。 | | | |