|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验6 | **实验名称** | UDP |
| **姓名** | 杨伟康 | **学号** | 202200201095 |
| **班级** | 网安班 | **成绩** | （空着） |
| 1. **实验目的**   我们来详细看一下UDP（用户数据报协议）。UDP是一种在互联网上广泛使用的传输协议，当不需要可靠性时，它可以作为TCP的替代方案。这部分内容在您的课本的6.4节中有所介绍。在进行本实验之前，请回顾一下该部分内容 | | | |
| 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。。  ifconfig / ipconfig：这个实验室使用“ipconfig”（Windows）或“ifconfig”（Mac/Linux）命令行工具来检查你的计算机网络接口的状态。 | | | |
| 1. **实验内容** 2. Capture a Trace. 3. Inspect the Trace 4. Message Structure 5. UDP Usage | | | |
| 1. **实验过程**   Step 1: Capture a Trace.  启动Wireshark并使用“udp”过滤器开始捕获。您的捕获窗口应该是  类似于下面的图片，除了我们的突出显示。选择CN5E实验室的接口  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    Step 2: Inspect the Trace  源端口（Source Port）：这是发送UDP消息的端口。它以一个数字和一个可能的文本名称给出；文本名称是给那些已注册用于特定应用程序的端口值。    目的端口（Destination Port）：这是UDP消息的目的端口号和可能的名称。端口是UDP中唯一的寻址形式。计算机在较低层的IP层中通过IP地址进行标识。    长度（Length）：UDP消息的长度。    校验和（Checksum）：消息上的校验和，用于验证其内容。从您的计算机发送的UDP消息的校验和是否为0，并且被标记为不正确？在某些计算机上，操作系统软件在发送数据包时，会将校验和留空（即零），由网络接口卡（NIC）计算并填充。这被称为协议卸载（protocol offloading）。它发生在Wireshark看到数据包之后，这导致Wireshark认为校验和错误，并用不同的颜色标记它以表示问题。如果发生这种情况，您可以告诉Wireshark不要验证校验和，以消除这些错误。从Wireshark菜单中选择“首选项（Preferences）”，并展开“协议（Protocols）”区域。在列表中查找直到找到UDP。取消选中“如果可能，验证校验和（Validate checksum if possible）”。    就是这样。UDP报头对于不同的消息有不同的值，但如您所见，它简短而简洁。消息的其余部分是UDP有效载荷，它通常标识它所携带的高层协议，例如DNS或RTP。    Step 3: UDP Message Structure  为了检查您对UDP的理解，请绘制一个您观察到的UDP消息结构图。它应显示IP标头、UDP标头和UDP有效负载的位置。在UDP标头中，显示您可以使用Wireshark观察到的每个UDP字段的位置和大小。您的图可以简单地显示消息显示为细长矩形。  尽量不要在文本中看到UDP段的图形；事后检查以进行记录和调查任何差异。要计算大小，请注意当您单击中间面板中的协议块时（块本身，而不是“+”扩展器），那么Wireshark将在在下面板中分组，并在窗口底部显示长度。  长度（Length）字段包括什么？ 是仅UDP有效载荷，还是包括UDP有效载荷和UDP报头，或者还包括更低层的报头？  **答案：长度（Length）字段包括UDP有效载荷和UDP报头的总长度（以字节为单位），但不包括更低层（如IP层）的报头。**  UDP校验和的长度是多少位？  **答案：UDP校验和的长度是16位（即2字节）。**  整个UDP报头的长度是多少字节？  **答案：整个UDP报头的长度是8字节。它包含源端口（2字节）、目的端口（2字节）、长度（2字节）和校验和（2字节）。**  提交内容：提交您绘制的UDP消息的图示以及上述问题的答案。  在这里插入图片描述  Step 4: UDP Usage  为了更全面地了解UDP，我们将探讨UDP作为应用程序传输层在实际中是如何被使用的。从IP开始，即下一个更低的协议层，我们可以考虑几个问题。  第一个问题是IP如何知道其上一层协议是UDP。答案是IP报头中有一个协议字段，该字段包含了这个信息。  给出IP协议字段中标识上层协议为UDP的值。  答案：IP协议字段中标识上层协议为UDP的值是17。  第二个问题是UDP消息在IP层通常是如何寻址的。您可能会惊讶地发现，在您的跟踪中，UDP消息并非都来自您的计算机或仅发送给您的计算机。您可以通过对“源”和“目的”列进行排序来查看这一点。如果启用了网络层名称解析，源和目的地将是域名；否则，它们将是IP地址。（您可以使用“视图”菜单并选择“名称解析”来切换此设置。）您可以使用“ipconfig”命令（Windows）或“ifconfig”命令（Mac/Linux）来查找您计算机的IP地址。只需在终端窗口中键入此命令，并查找主接口的IPv4地址即可。下面给出了示例。  =    您可能会发现UDP消息中源或目的IP地址并非您计算机IP地址的原因是，UDP被广泛用于系统协议的一部分。这些协议经常使用广播和多播地址向所有感兴趣的本地计算机发送消息。在我们的跟踪中，我们发现了DNS（域名系统）、MDNS（使用IP多播的DNS流量）、NTP（用于时间同步）、NBNS（NetBIOS流量）、DHCP（用于IP地址分配）、SSDP（服务发现协议）、STUN（NAT穿越协议）、RTP（用于传输音频和视频样本）等。  您的跟踪中可能还有其他您未曾听说过的协议，这是正常的，因为存在大量的协议。为了乐趣，您可以在网上查找它们。  检查UDP消息，并给出当您的计算机既不是源IP地址也不是目的IP地址时所使用的目的IP地址。（如果您的跟踪中只有您的计算机作为源或目的IP地址，则可以使用提供的跟踪。）  最后，让我们看一下典型UDP消息的长度。我们知道UDP消息的大小可以大致达到64K字节。但是，在浏览时您应该会看到，大多数UDP消息都远小于这个最大值，以便UDP消息能够适合单个数据包。  您的跟踪中UDP消息的典型大小是多少？  提交内容：提交您对上述问题的答案。    Explore on your own  **我们鼓励您继续自行探索，但UDP的内容并不多。相反，您可以检查基于UDP的应用程序的流量，以查看数据包大小和丢失率。Voice-over-IP（VoIP）及其伴随协议如RTP（实时传输协议）是很好的候选者。同样，您可以探索流媒体和实时应用程序，以查看哪些使用UDP作为传输协议，哪些使用TCP作为传输协议。** | | | |
| **四．实验心得**  学习UDP后，我深刻体会到其在网络协议中的重要性。UDP以其简单、高效的特点，广泛应用于对实时性要求较高但不要求数据绝对可靠的场景，如VoIP、视频流等。通过了解UDP的数据包结构和传输机制，我认识到其在处理大量小数据包时的高效性，同时也意识到其不提供错误检测和数据重传服务的局限性。这次学习不仅加深了我对网络协议栈的理解，还激发了我对实际应用中协议选择和优化策略的思考 | | | |