|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验8 | **实验名称** | DNS |
| **姓名** | 杨伟康 | **学号** | 202200201095 |
| **班级** | 网安班 | **成绩** | （空着） |
| 1. **实验目的**   DNS（域名系统）是一种系统和协议，用于将域名翻译成IP地址以及其他信息。学习DNS相关内容 | | | |
| 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。。  dig： 本实验使用dig工具来发出DNS请求并观察DNS响应。dig是一个灵活的命令行工具，用于查询远程DNS服务器，它取代了较旧的nslookup程序。  Browser: 可以使用任何Web浏览器来查找或获取页面作为工作负载。 | | | |
| 1. **实验内容** 2. Manual Name Resolution 3. Capture a Trace 4. Inspect the Trace 5. Details of DNS Messages 6. DNS Response Time | | | |
| 1. **实验过程**   Network Setup  在典型的网络中，您的计算机会联系本地DNS名称服务器，以将域名解析为IP地址。本地名称服务器可能是您公司网络中的另一台计算机、您互联网服务提供商(ISP)的计算机，或您的无线接入点(AP)。它通过与遍布互联网的远程DNS名称服务器交换一系列消息来执行解析。设置如以下图所示。    我们假设实验采用这种设置，它有一个重要的含义：我们在计算机上收集的跟踪将看到我们计算机与本地名称服务器之间的交换，但看不到本地名称服务器与远程名称服务器之间的交换。  Step 1: Manual Name Resolution  在我们查看计算机如何使用DNS之前，我们将先了解本地名称服务器如何解析DNS名称，即我们将与远程名称服务器进行交互。为了完成这个练习，您将扮演本地名称服务器的角色，并使用dig工具向远程名称服务器发出请求。  选择一个要解析的域名，比如您的Web服务器的域名。我们将使用www.uwa.edu.au作为示例。通过搜索网络找到其中一个根名称服务器的IP地址。例如，维基百科上关于根名称服务器的文章就包含了从a到m的根名称服务器的IP地址。这些中的任何一个都可以，因为它们包含复制的信息。您需要这些信息来开始名称解析过程，并且名称服务器会在其配置中提供这些信息。  使用dig向根名称服务器发出请求，以执行解析的第一步。您假设自己没有缓存信息，这些信息将允许您在根以下开始解析。dig命令的格式是“dig @aa.bb.cc.dd domainname”。它指示dig向给定IP地址（或名称）的名称服务器发送针对给定域名的请求。在下图中，我们使用dig向IP地址为198.41.0.4的“a”根名称服务器发送请求，以解析我们的示例Web服务器，即“dig @198.41.0.4 www.uwa.edu.au”。根名称服务器的回复不会提供完整的名称解析，但它会告诉我们更接近拥有您需要联系的信息的名称服务器。在这种情况下，是了解“.au”域的名称服务器。提供了多个名称服务器作为备选方案，并且回复还贴心地包括了它们的IP地址；我们可以看到IPv6地址以及IPv4地址。  继续使用dig来完成解析过程。当您有多个选项可以选择时，请优先选择IPv4名称服务器，并按字母顺序选择第一个。如果该名称服务器有多个IP地址，请选择数值上最小的IP地址。在图中，IP地址为58.65.254.73且对“au.”具有权威性的名称服务器是接下来要联系的远程名称服务器。即使没有这些打破平局的规则，您也可以完成解析，并且很可能会获得相同的结果，因为DNS信息是复制的。这些规则是为了让进行实验室操作的每个人都遵循相同的路径。请将这些dig命令保存好，因为您将在下一步捕获跟踪时重复它们。    Step 2: Capture a Trace  按照以下步骤捕获浏览器发出DNS请求的跟踪信息；或者，您也可以使用提供的跟踪信息。现在我们已经熟悉了名称解析的过程，接下来我们将检查DNS流量的详细信息。为了生成DNS流量，您将需要重复执行dig命令并浏览网站。  关闭所有不必要的浏览器标签页和窗口。浏览网站时，浏览器会解析域名以连接到远程服务器，从而产生DNS流量。我们最初希望最小化浏览器活动，以便仅捕获预期的DNS流量。  启动Wireshark，并使用“udp port 53”作为过滤器开始捕获。我们使用此过滤器是因为DNS没有简写形式，但DNS通常通过UDP端口53进行传输。您的捕获窗口应与下图类似（除了我们高亮的部分）。选择用于捕获的接口，即您计算机用于连接到互联网的主要有线或无线接口。如果不确定，请猜测，并在捕获不成功时稍后重新检查此步骤。取消选中“以混杂模式捕获数据包”。此模式有助于监听广播网络上其他计算机发送/接收的数据包。但我们只想记录发送/接收到您计算机的数据包。将其他选项保留为默认值。如果存在捕获过滤器，则用于防止捕获您的计算机可能发送或接收的其他流量。在Wireshark 1.8中，捕获过滤器框直接位于选项屏幕上，但在Wireshark 1.9中，您可以通过双击接口来设置捕获过滤器。  这里使用默认提供的    Step 3: Inspect the Trace  为了探索DNS数据包的详细信息，请选择一个DNS查询并展开其“域名系统”块（使用“+”展开器或图标）。您的显示应该与我们在图中所示的类似，其中包含一系列具有DNS协议的数据包。首先出现的数据包应该对应于您的dig命令，随后是浏览器产生的DNS流量。我们已经选择了第一个DNS消息。    查找以下详细信息：  • DNS块位于IP和UDP块之后。这是因为DNS消息是在IP数据包内的UDP段中传输的。您会看到名称服务器使用的UDP端口是53。    • DNS头部以一个事务ID开始，该ID用于将请求和相应的回复关联起来——它们都携带相同的事务ID。  • 接下来是一组可以展开的标志。它们指示DNS消息是查询还是响应，以及其他详细信息。  • 然后是查询、回答、授权和附加记录的数量。这些字段构成了头部的结尾。  • 在DNS头部之后，消息的其余部分由指定数量的查询、回答、授权和附加记录组成。通常只有一个查询——针对我们正在查找的域名的IP地址——但可能有许多其他记录。这些记录被分组在部分中，例如包含所有授权记录的授权部分。每个查询都有一个类型代码，指示所请求的记录类型，无论是IP地址还是其他类型。其他每条记录也有一个类型代码，指示它是否携带主机的IP地址、名称服务器的名称或其他内容。单个记录的格式取决于其类型。整个DNS消息被设计为适合一个UDP消息。  • Wireshark可能会显示其他信息，如携带此请求响应的数据包编号或DNS交换的响应时间，但这是派生信息。它实际上并没有在任何数据包上携带。  重复上述步骤以查看DNS响应。您应该在此消息中看到更大的一组记录；虽然DNS查询主要用于携带查询，但DNS响应通常会返回一组有用的信息。    Step 4: Details of DNS Messages   1. **事务ID（Transaction ID）的长度**： 事务ID在DNS消息中通常是16位（2字节）长。由于它是16位的，这意味着它可以有从0到65535（即2^16-1）的不同值。因此，在并发事务数量不是极端庞大的情况下，两个并发事务使用相同事务ID的可能性相对较低，但并非不可能。然而，在实际情况中，由于DNS客户端（如dig命令或浏览器）会合理管理其事务，因此这种情况很少发生。 2. **表示DNS消息是查询还是响应的标志位**： DNS消息中的QR（Query/Response）标志位用于指示消息是查询还是响应。QR标志位位于DNS头部的第2字节（从0开始计数）的第0位（最右边的位）。如果QR位被设置为0，则表示该消息是一个查询；如果设置为1，则表示该消息是一个响应。 3. **整个DNS头部的长度**： 整个DNS头部的长度不是固定的，但它至少包含12字节的固定部分，这些部分包括事务ID（2字节）、标志（2字节）、问题计数（2字节）、回答RR计数（2字节）、授权RR计数（2字节）和附加RR计数（2字节）。然而，DNS头部还可能包含可选的字段，如EDNS0（扩展DNS 0）信息，这会增加头部的长度。在Wireshark中，当您选择DNS头部时，可以在底部的状态行或详细信息面板中看到实际的头部长度。要准确计算，请确保选择整个DNS头部，并查看Wireshark提供的长度信息。   现在检查您发出的dig DNS查询的响应。初始响应应该提供了更接近名称服务器的另一个名称服务器，但并非最终答案。您会发现它在查询部分包含了原始查询。它还将包含记录，这些记录既有接下来要联系的名称服务器的名称，也有这些名称服务器的IP地址。这一系列中的最终响应将包含域名的IP地址——这是查询的答案。  查看DNS响应消息的主体，并回答以下问题：  对于初始响应，名称服务器的名称是在哪个部分携带的？携带名称服务器名称的记录的类型是什么？  答：在“回答”部分（Answer Section）会携带名称服务器的名称。这些记录的类型是NS（Name Server）记录。  同样地，名称服务器的IP地址是在哪个部分携带的，携带IP地址的记录的类型是什么？  答：在“回答”部分（Answer Section）也会携带名称服务器的IP地址。但直接携带IP地址的记录类型通常是A（IPv4地址）或AAAA（IPv6地址）记录，具体取决于IP地址的类型。然而，在NS记录的“附加”部分（Additional Section）中，可能会找到与NS记录相对应的A或AAAA记录，这些记录提供了NS记录的IP地址。  对于最终响应，域名的IP地址是在哪个部分携带的？  答：在最终响应中，域名的IP地址是在“回答”部分（Answer Section）携带的。这些记录的类型通常是A（IPv4地址）或AAAA（IPv6地址）记录，具体取决于查询的上下文和域名的配置。  Step 5: DNS Response Time  为了结束这个实验，我们将查看浏览器发出的DNS查询的DNS响应时间。这是您正常的DNS使用情况，其中您的计算机发送一个查询并在响应中接收答案。响应时间是指从您的计算机向本地名称服务器发送查询到从本地名称服务器接收响应之间的延迟。这个时间包括如果答案没有被缓存，则本地名称服务器与远程名称服务器联系所需的时间。由于这个响应时间可能会延迟到网站的连接，因此应该尽可能小。  请按照以下步骤生成DNS响应时间的“IO图表”。IO图表是Wireshark在“统计”菜单下的一个标准功能。默认情况下，此图表显示随时间变化的数据包速率。我们将对其进行调整，以通过以下更改在跟踪中显示DNS响应时间：  • 在x轴上，调整刻度间隔和每刻度的像素数以进行查看。刻度间隔应该足够小，以便能够查看跟踪中的行为。对于您的跟踪，一秒钟可能是一个不错的选择。每刻度的像素数可以进行调整，以使图表更宽或更窄，以填满窗口；您也可以调整窗口的宽度。  • 在y轴上，将单位更改为“高级”。默认是“数据包/刻度”。“高级”是一个特殊关键字，将允许我们访问不同的数据值来绘图。选择它后，将出现一个新的“Calc:”框，让我们可以指定数据值。  • 在计算框中输入“dns.time”，并将下拉菜单设置为“MAX()”。dns.time是Wireshark根据查询和响应消息计算得出的虚拟字段。它与DNS响应一起显示，并给出DNS响应时间。选择“MAX()”将使我们能够看到每个刻度间隔中最大的DNS响应时间，以便我们可以发现异常值。“AVG(\*)”也是一个合理的选择。  • 按Enter键，并在必要时点击“图形”按钮。您可能需要执行此操作以查看生成的DNS响应时间IO图表。这将提供一个直观的视图，显示在整个跟踪过程中DNS响应时间的分布和可能的延迟问题    如果您查看由浏览器引起的DNS流量，您可能会看到比由dig命令引起的DNS流量更广泛的行为。这些行为可能包括新类型的记录，如CNAME（规范名称，当一台机器以多个名称为人所知时，提供有关别名的信息）、表明名称不存在的答案等等。  Explore on your own  **MX记录和AAAA记录的主要用途是什么？**  MX记录的主要用途是查找特定域的邮件服务器。当电子邮件系统需要发送或接收来自该域的电子邮件时，它会查询MX记录以找到正确的邮件服务器。  AAAA记录的主要用途是查找特定域的IPv6地址。随着IPv6的普及，AAAA记录变得越来越重要，因为它们允许设备与只支持IPv6的网络上的其他设备通信。  **Google Public DNS相对于其他DNS提供商的优势可能是什么？**  Google Public DNS可能比其他DNS提供商更快，因为它在全球范围内拥有多个服务器位置，可以提供更快的响应时间。  它还可能提供更高的隐私和安全性，因为它不会记录用户的IP地址或与用户查询相关联的其他个人信息。  Google的技术实力意味着其DNS系统可能更稳定且故障更少。  **反向DNS查找为什么常被用作安全检查？**  反向DNS查找常被用作安全检查，因为它们可以帮助识别潜在的欺诈行为或伪装。如果IP地址的反向DNS查找结果与预期的域名不匹配，那么这可能是一个警告信号，表明该IP地址可能正在被用于恶意目的。  此外，通过反向DNS查找，管理员可以验证网络上的设备是否正确地配置了其域名信息，这有助于维护网络的整体健康和安全。 | | | |
| **四．实验心得**  学习DNS的过程让我深刻认识到它在互联网架构中的重要性。DNS作为互联网的“电话簿”，将人类可读的域名转换为机器可识别的IP地址，极大地简化了网络访问的复杂性。通过学习，我不仅掌握了DNS的基本概念和查询原理，还了解了不同类型的DNS记录及其作用。此外，探索Google Public DNS和DNSSEC等高级特性，让我对DNS的安全性和性能优化有了更深入的理解。这次学习不仅拓宽了我的知识面，也激发了我对网络技术的浓厚兴趣。未来，我希望能继续深入探索更多网络领域的奥秘。 | | | |