|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验5 | **实验名称** | ARP |
| **姓名** | 杨伟康 | **学号** | 202200201095 |
| **班级** | 网安班 | **成绩** | （空着） |
| 1. **实验目的**   为了了解ARP（地址解析协议）是如何工作的。ARP是一个关键的粘合剂协议，用于将以太网和IP连接在一起。它在你的教材的第5.6.4节中有所介绍。在做这个实验室之前，请回顾一下该文本部分。 | | | |
| 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。。  ARP：这个实验室使用“arp”命令行工具来检查和清除你的计算机上ARP协议所使用的缓存。  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。  route / netstat：这个实验室使用“route”或“netstat”命令行工具来检查你的计算机所使用的路由。一个关键的路由是默认路由（或到前缀0.0.0.0的路由），它使用默认网关来访问互联网的远程部分。  浏览器：这个实验室使用一个网页浏览器来查找或获取页面作为工作负载。任何网页浏览器都可以。 | | | |
| 1. **实验内容** 2. Capture a Trace. 3. Inspect the Trace 4. ARP request and reply 5. Details of ARP over Ethernet | | | |
| 1. **实验过程**   Network Setup  我们想要观察ARP协议的实际操作。请回想一下，ARP用于查找与本地IP地址相对应的以太网地址，你的计算机想要向该地址发送数据包。本地IP地址的一个典型例子是本地路由器或默认网关的IP地址，它连接你的计算机到互联网的其余部分。你的计算机会将这些转换缓存在ARP缓存中，因此ARP协议只需要偶尔使用来进行转换。从你的计算机的角度来看，设置如下所示    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    1. 使用ifconfig / ipconfig命令找到你的计算机主要网络接口的以太网地址。你将在后续的分析中需要这个地址。在Windows上，打开命令行窗口并输入“ipconfig /all”。    2. 使用netstat / route命令找到你的计算机用来连接到互联网其余部分的本地路由器或默认网关的IP地址。  3. 启动Wireshark，并使用“arp”作为过滤器开始捕获。    4. 当捕获开始时，使用“arp”命令清除ARP缓存中的默认网关。使用“arp –a”命令将显示ARP缓存的内容，以便你可以运行“arp”。你应该能看到默认网关的IP地址的条目。要清除这个条目，请使用具有不同参数的arp命令（“arp –d”在Windows上，“arp –d –a”在Mac上，“arp –d xx.xx.xx.xx”，其中xx.xx.xx.xx是Linux上默认网关的IP地址）。运行arp的这种用法需要管理员权限，因此你可能需要在Windows上以特权用户身份运行，或者在Linux/Mac上发出“sudo arp –d xx.xx.xx.xx”命令。请注意，该命令应该能够无错误地运行，但如果你使用“arp –a”检查，ARP条目可能看起来并没有清除。这是因为你的计算机在需要向远程IP地址发送数据包时会立即发送ARP数据包以重新填充这个条目，而且由于计算机上的后台活动，这可能会很快发生。  5.现在你已经清除了ARP缓存，使用你的网络浏览器获取一个远程页面。这将导致ARP查找默认网关的以太网地址，以便发送数据包。这些ARP数据包将被Wireshark捕获。你可以清除ARP缓存并多次获取文档。希望还能捕获到本地网络上其他计算机发送的其他ARP数据包。如果本地网络上有其他计算机，那么这些数据包很可能存在。事实上，如果你的计算机很忙，本地网络很广泛，那么你可能会捕获到许多ARP数据包。当ARP数据包发送到广播地址时，将捕获其他计算机的ARP流量，因为在这种情况下，它们是要发送给所有计算机的，包括你正在运行Wireshark的那台计算机。由于ARP活动发生得比较慢，你可能需要等待最多30秒才能观察到一些背景ARP流量。  6. 一旦你捕获了一些ARP流量，就停止捕获。你将需要这个跟踪记录，加上你的计算机的以太网地址和默认网关的IP地址，以进行下一步操作。  Step 2: Inspect the Trace  为您的计算机以太网地址设置显示过滤器。您可以通过在Wireshark窗口顶部附近的空白“Filter:”框中输入表达式并点击“Apply”来实现。  设置过滤器内容：eth.addr==00:25:64:d5:10:8b    找到并选择针对默认网关的ARP请求，并检查其字段。ARP数据包有两种类型，一种是请求，另一种是回复，我们将依次查看它们。ARP请求的“Info”行将以“Who has …”开头。您需要查找其中一个数据包，该数据包请求默认网关的MAC地址，例如“Who has xx.xx.xx.xx …”，其中xx.xx.xx.xx是您的默认网关的IP地址。您可以点击Address Resolution Protocol（地址解析协议）块旁边的加号展开器或图标来查看字段：  • 硬件类型和协议类型被设置为常量，告诉我们硬件是Ethernet（以太网），协议是IP。这与ARP从IP地址到以太网地址的转换相匹配。  • 硬件大小和协议大小分别被设置为6和4，这是以太网和IP地址的字节大小。  • 操作码字段告诉我们这是一个请求。CN5E Labs (1.0) © 2012 D. Wetherall 8  • 接下来是四个关键字段，即发送者的MAC（以太网）和IP地址，以及目标MAC（以太网）和IP地址。这些字段在可能的情况下会被填充。对于请求，发送者知道他们自己的MAC和IP地址并填写它们。发送者也知道目标IP地址——这是想要查找以太网地址的IP地址。但是发送者不知道目标MAC地址，所以不会填写它。    接下来，选择一个ARP回复并检查其字段。回复将回答一个请求，并带有形如“xx.xx.xx.xx is at yy:yy:yy:yy:yy:yy”的“Info”行：  • 硬件类型和协议类型以及大小与之前设置的一样。  • 操作码字段有一个不同的值，告诉我们这是一个回复。  • 接下来是四个关键字段，即发送者的MAC（以太网）和IP地址，以及目标MAC（以太网）和IP地址，与之前的顺序相同。这些字段与相应的请求相反，因为原来的目标是新的发送者（反之亦然）。现在这些字段应该都填写完整了，因为两台计算机都提供了它们的地址。    Step 3: ARP request and reply  为了展示您对ARP交换的理解，请绘制一幅图，展示您计算机与默认网关之间发送的ARP请求和回复数据包。请根据您计算机为默认网关执行ARP查询的情况来绘制。将其中一个数据包标记为请求，另一个标记为回复。为每个数据包标出发送者和目标的MAC和IP地址；您可以使用Wireshark来检查数据包以获取这些值。最后，在您的图上圈出所寻求的以太网地址，以显示它在交换中的来源。  提交：提交您绘制的ARP交换图。  在这里插入图片描述  Step 4: Details of ARP over Ethernet  为了查看ARP的更多细节，请检查ARP请求和ARP回复以回答以下问题：  用于指示请求的操作码是什么？回复的操作码又是什么？  ARP请求头的大小是多少？回复的ARP头大小又是多少？  在请求中，对于未知的目标MAC地址，携带了什么值？  用于指示请求的操作码是1（通常表示为十六进制数0x01）。回复的操作码是2（通常表示为十六进制数0x02）。  ARP请求头的大小（不包括以太网帧头部和可能的填充字节）通常是28字节。这个大小包括ARP头部的所有字段，如硬件类型、协议类型、硬件地址长度、协议地址长度、操作码、发送方硬件地址、发送方协议地址、目标硬件地址（在请求中通常为0）和目标协议地址。  在ARP请求中，对于未知的目标MAC地址，目标硬件地址字段（Target Hardware Address）被设置为全零（通常是6个连续的十六进制数00:00:00:00:00:00），因为发送方在发送ARP请求时还不知道目标设备的MAC地址。目标协议地址字段（Target Protocol Address）则包含目标设备的IP地址，这是发送方想要解析为MAC地址的IP地址。  ARP数据包被封装在以太网帧中，以太网头部字段的值被选择以支持ARP。例如，你可能会好奇ARP请求数据包是如何被发送到目标计算机以便它能够回复并告诉请求者其MAC地址的。答案是ARP请求（通常）在以太网层以广播方式发送，以便被包括目标在内的本地网络上的所有计算机接收。特别地看一下请求的目标以太网地址：它被设置为ff:ff:ff:ff:ff:ff，即广播地址。因此，目标接收请求并识别出它是消息的预定接收者；其他接收到请求的计算机知道这不是给它们的。只有目标会用一个回复来响应。然而，任何接收到ARP数据包的人都可以从中学习到一个映射关系：即发送者MAC和发送者IP对。  检查ARP请求和回复以回答以下问题：  哪个以太网类型值表示ARP是更高层的协议？  ARP回复是广播的（像ARP请求一样）还是不是？  以太网类型值表示ARP是更高层的协议是0x0806。这个值在以太网帧的头部中，用于指示负载数据的类型，当该值为0x0806时，表示负载数据是ARP协议的数据包。  ARP回复不是广播的，与ARP请求不同。ARP请求是广播发送的，即目的MAC地址为ff:ff:ff:ff:ff:ff，以便让局域网内的所有主机都能收到并检查是否与自己的IP地址匹配。然而，当某台主机识别到ARP请求中的目标IP地址与自己的IP地址匹配时，它会生成一个ARP回复，该回复是单播发送的，即目的MAC地址为ARP请求中的源MAC地址，确保只有发送ARP请求的主机能够收到回复。  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：**  **• 其他计算机广播的ARP请求。本地网络上的其他计算机也在使用ARP。由于请求是广播发送的，您的计算机将接收到它们的请求。**  **• 您的计算机发送的ARP回复。如果另一台计算机恰好需要ARP请求您的计算机的IP地址，那么您的计算机将发送一个ARP回复来告诉它答案。**  **回答：是的，这些都是ARP协议在网络中的常见使用场景。在局域网中，ARP协议用于将IP地址解析为MAC地址，以便进行通信。当一台计算机需要知道另一台计算机的MAC地址时，它会发送一个ARP请求，该请求会被广播到整个局域网。所有接收到这个ARP请求的计算机都会检查请求的IP地址是否与自己匹配，如果不匹配则忽略该请求；如果匹配，则发送一个ARP回复，包含自己的MAC地址。因此，本地网络上的所有计算机都可能接收到ARP请求，但只有目标计算机会发送ARP回复。同样地，当其他计算机需要知道您的计算机的MAC地址时，您的计算机也会发送ARP回复来提供相关信息。** | | | |
| **四．实验心得**  学习ARP协议并通过Wireshark进行实践，我深刻体会到了网络底层的奥秘和复杂性。ARP作为地址解析协议，在网络通信中扮演着至关重要的角色。通过Wireshark观察ARP请求和回复，我直观地看到了数据包的传输过程，理解了IP地址到MAC地址的映射机制。这次学习不仅增强了我的网络知识，还锻炼了我的实践能力，让我对网络通信有了更深入的理解。我深感网络世界的博大精深，期待未来能继续深入探索。 | | | |