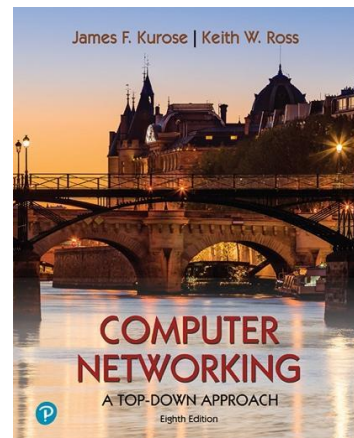


维尔哈克实验室： DNS v8.1

计算机网络的补充部分：一个自上而下的版本
接近，第8版，J. F. Kurose和K. W. 罗斯

“告诉我，我忘了。给我看看，我记得了。让我参与进来
和我的理解。”中国的谚语

©2005-2021，J. F. Kurose和K. W. Ross，版权所有



如文本1第2.4节所述，域名系统（DNS）进行翻译主机名到IP地址，在互联网基础设施中发挥着关键作用。在这个实验室中，我们将仔细研究DNS的客户端。回想一下，客户机在DNS中的角色相对简单——客户机向查询发送到本地DNS服务器，然后接收响应。如图教科书中的2.19和2.20所示，由于分层DNS服务器通过递归或迭代解析DNS查询相互通信，客户端的DNS查询不可见。然而，从DNS客户机的角度来看，该协议非常简单——对本地DNS服务器制定一个查询，并从该服务器接收一个响应。

在开始这个实验室之前，您可能需要通过阅读的第2.4节来回顾DNS语篇特别是，您可能希望查看本地DNS服务器、DNS缓存、DNS记录和消息以及DNS记录中的TYPE字段上的材料。

1. 查询域名

让我们通过检查nslookup命令来开始调查DNS将调用底层的DNS服务来实现其功能。nslookup命令在大多数微软、苹果iOS和Linux操作系统中都适用。要运行ns查找，您只需在DOS窗口、Mac OS终端窗口或Linux shell的命令行中输入nslookup命令。

在其最基本的操作中，ns查找允许运行ns查找的主机查询任何查询为DNS记录指定的DNS服务器。查询的DNS服务器可以是根DNS服务器、顶级域（TLD）DNS服务器、权威DNS服务器或中间DNS服务器（有关这些术语的定义，请参阅教科书）。例如，

1 参考数字和部分是为我们文本的第8版，计算机网络，一个自上而下的方法，第8版，J. F. Kurose和K. 罗斯，艾迪生-韦斯利/皮尔森，2020年。我们为这本书建立的网站是http://gai.a.cs.umass.edu/kurose_ross，你会在那里发现很多有趣的开放材料。

ns查找可用于检索“=a型”DNS记录，该记录将主机名（例如，www.nyu.edu）映射到它的IP地址。要完成此任务，nslookup向指定的DNS服务器发送DNS查询（如果没有指定特定的Dnslookup的默认DNS运行主机的本地DNS服务器），从该DNS服务器接收DNS响应，并显示结果。

让我们来看看吧！我们将首先在Linux命令上运行ns查找
让我们来看看新世界吧。美国的.edu主机位于马萨诸塞大学（UMass）校园的CS系，本地名称服务器被命名
primo.cs.umass.edu（其IP地址为128.119.240.1）。让我们尝试最简单的ns查找：

```
newworld.cs.umass.edu> nslookup www.nyu.edu
Server:      128.119.240.1
Address:     128.119.240.1#53

Non-authoritative answer:
www.nyu.edu  canonical name = WEB.GSLB.nyu.edu.
Name:   WEB.GSLB.nyu.edu
Address: 216.165.47.12
Name:   WEB.GSLB.nyu.edu
Address: 2607:f600:1002:6113::100
```

图1：基本的nslookup命令

在本例中，nslookup命令有一个参数，一个主机名（www.nyu.edu）。也就是说，这个命令是说：“请把主机www.nyu的IP地址发送给我。”edu。如屏幕截图所示，该命令的响应提供了两条信息：（1）提供答案的DNS服务器的名称和IP地址——在这里是马萨诸塞大学的本地DNS服务器；（2）答案本身，即www.nyu的规范主机名和IP地址。edu。您可能已经注意到，为www.nyu.edu提供了两个名称/地址对。第一个(216.165.47.12)是一个IPv4地址，以熟悉的点线十进制符号表示；第二个地址(2607:f600:1002:6113::100)是一个更长、更复杂的IPv6地址。我们将在第4章的后面了解IPv4和IPv6及其两种不同的寻址方案。现在，让我们只关注我们更舒适（也更常见）的IPv4世界²。

尽管响应来自本地DNS服务器(其IP地址为128.119.240.1)在马萨诸塞州，很有可能这个本地DNS服务器迭代地联系其他几个DNS服务器以获得答案，如教科书第2.4节所述。

除了使用nslookup查询DNS的“=a型”记录外，我们还可以使用查询“TYPE=NS”记录，该记录返回权威DNS服务器的主机名（及其IP地址），该服务器知道如何获取权威服务器域中的主机的IP地址。

² 对于Mac OS系统，如果你想只在IPv4世界工作：系统首选项->网络。然后选择您的活动界面（例如，Wi-Fi）和高级->TCP/IP。然后选择配置IPv6下拉菜单，并将其设置为“仅链接本地”或“关闭”。

```

newworld.cs.umass.edu> nslookup -type=NS nyu.edu
Server:      128.119.240.1
Address:     128.119.240.1#53

Non-authoritative answer:
nyu.edu nameserver = ns2.nyu.org.
nyu.edu nameserver = ns4.nyu.edu.
nyu.edu nameserver = ns1.nyu.net.

Authoritative answers can be found from:
ns2.nyu.org      internet address = 128.122.0.76
ns1.nyu.net      internet address = 128.122.0.8
ns4.nyu.edu      internet address = 216.165.87.102
ns4.nyu.edu      has AAAA address 2607:f600:2001:6100::135

```

图2：使用nslookup查找纽约大学的权威名称服务器。edu域

在图2中的示例中，我们已经使用选项“-type=NS”和调用了ns查找域“纽约大学”。edu”。这将导致ns查找将类型-NS记录的查询发送到默认的本地DNS服务器。也地说，查询是，“请将权威DNS的主机名发给我。”edu”。（当不使用-type选项时，nslookup将使用默认值，即查询类型为A的记录。）答案，显示在上面的屏幕截图中，首先指示提供答案的DNS服务器（这是地址为128.119.240.1的默认本地UMass DNS服务器。1）以及三个纽约大学的DNS名称服务器。这些服务器实际上都是纽约大学校园内主机的权威DNS服务器。然而，nslookup还表明答案是“非权威的”，这意味着这个答案来自某个服务器的缓存，而不是来自权威的NYU DNS服务器。最后，答案还包括纽约大学权威DNS服务器的IP地址。（尽管nslookup生成的类型-NS查询没有显式地要求IP地址，本地DNS服务器“免费”返回这些查询，nslookup显示结果。）

nslookup除了“-type=NS”之外还有许多可能需要的附加选项

探索。这里有一个网站的屏幕截图经常流行的nslookup使用：

<https://www.cloudns.net/blog/10-most-used-nslookup-commands/>和[这里是ns查找的“手册页”](https://linux.die.net/man/1/nslookup)：<https://linux.die.net/man/1/nslookup>。

最后，我们有时可能会对发现相关的主机的名称感兴趣

使用给定的IP地址，即图1所示的查找相反（其中主机的名称已知/指定，并返回主机的IP地址）。ns查找也可以用于执行这种所谓的“反向DNS查找”。例如，在图3中，我们指定了一个IP地址作为nslookup参数（128.119.245.12）和nslookup返回具有该地址（gaia.美国的。Edu）

```

[kurose@MacBook-Pro-6 ~ % nslookup 128.119.245.12
Server:      75.75.75.75
Address:     75.75.75.75#53

Non-authoritative answer:
12.245.119.128.in-addr.arpa      name = gaia.cs.umass.edu.

Authoritative answers can be found from:

```

图3：使用ns查找来执行“反向DNS查找”

现在我们已经提供了nslookup的概述，是时候测试它了
你自己执行以下操作（并写下结果³）。如果你在课堂的一部分做这个实验室，你的老师会提供如何提交作业的细节，无论是书面的还是LMS。如果您无法运行nslookup命令或正在使用LMS回答这个问题，图4显示了在问题1和问题4中执行ns查找的屏幕截图，这将允许您回答下面的问题。

1. 运行ns查找以获取印度人的web服务器的IP地址
印度孟买理工学院：www.iitb.交流。www.iitb的IP地址是什么。交流电。在
2. 提供答案的DNS服务器的IP地址是什么
上面问题1中的nslookup命令？
3. 上面问题1中的nslookup命令的答案是否来自一个权威的或非权威的服务器？
4. 使用ns查找命令来确定权威名称的名称
针对iit的服务器。ac。在这个领域。那个名字是什么？（如果有多个权威服务器，那么nslookup返回的第一个权威服务器的名称是什么）？如果您必须找到该权威名称服务器的IP地址，那么您将如何找到呢？

```
kurose@MacBook-Pro-6 ~ % nslookup www.iitb.ac.in
Server:      75.75.75.75
Address:     75.75.75.75#53

Non-authoritative answer:
Name:   www.iitb.ac.in
Address: 103.21.124.10

kurose@MacBook-Pro-6 ~ % nslookup -type=NS iitb.ac.in
Server:      75.75.75.75
Address:     75.75.75.75#53

Non-authoritative answer:
iitb.ac.in   nameserver = dns1.iitb.ac.in.
iitb.ac.in   nameserver = dns2.iitb.ac.in.
iitb.ac.in   nameserver = dns3.iitb.ac.in.
```

图4：使用nslookup查找www.iitb的IP地址。还有他们和他们的名字
针对iitb的权威名称服务器。交流电。在本领域内

2. 您的计算机上的DNS高速缓存

从对迭代的和递归的DNS查询解析的描述开始(图2.19和
2.20) 在我们的教科书中，您可能会认为必须每次都联系本地DNS服务器

³ 对于作者的课堂，当用手工作业回答以下问题时，学生有时需要打印出特定的包（参见介绍的线
鲨实验室解释如何做到这一点），并指出他们在包的哪里找到了回答问题的信息。他们通过用钢笔
标记纸上的副本，或用彩色字体的文本注释电子副本。还有供教师使用的学习管理系统（LMS）模
块，允许学生在线回答这些问题，并为这些线鲨实验室进行自动评分

http://gaia.cs.umass.edu/kurose_ross/lms.htm

应用程序需要从主机名转换为IP地址的时间。这在实践中并不总是正确的！

大多数主机（例如，您的个人计算机）保存最近检索到的DNS记录的缓存（有时被称为DNS解析器缓存），就像许多Web浏览器保存了由HTTP最近检索到的对象的缓存一样。当主机需要调用DNS服务时，该主机将首先检查所需的DNS记录是否驻留在此主机的DNS缓存中；如果找到该记录，主机甚至不会联系本地DNS服务器，而是使用此缓存的DNS记录。解析器缓存中的DNS记录最终将超时并从解析器缓存中删除，就像本地DNS服务器中缓存的记录（参见图2.19, 2.20）将超时一样。

您还可以显式地清除DNS缓存中的记录。这样做没有什么害处因此，这将意味着您的计算机下次需要使用DNS名称解析服务时需要调用分布式DNS服务，因为它不会在缓存中找到任何记录。在Mac计算机上，您可以在终端窗口中输入以下命令，以清除DNS解析器缓存：

```
sudo killall -HUP mDNSResponder
```

在Windows计算机上，您可以在命令提示符下输入以下命令：

```
ipconfig /flushdns
```

并在Linux计算机上，输入：

systemctl restart systemd-resolved

3. 用有线鲨鱼追踪DNS

现在我们已经熟悉了ns查找和清理DNS解析器缓存，我们是准备好去做一些严肃的事情了。让我们首先捕获由普通网络冲浪活动生成的DNS消息。

- . 如上所述，清除主机中的DNS缓存。
- . 打开Web浏览器并清除浏览器缓存。
- . 打开有线鲨鱼并进入ip.addr==<您的_IP_地址>到显示过滤器，其中<您的_IP_地址>是您的计算机的IPv4地址⁴。有了这个过滤器，有线鲨鱼只会显示来自或注定向您的主机的数据包。
- . 开始在有线鲨鱼中的数据包捕获。
- . 使用您的浏览器，请访问网页：http://gail.cs.umass.edu/kurose_ross/
- . 停止数据包捕获。

⁴ 如果您不确定如何找到您的计算机的IP地址，您可以在网上搜索有关您的操作系统的文章。
Windows 10信息在这里；Mac信息在这里；Linux信息在这里

如果您无法在实时网络连接上运行有线鲨鱼，您可以下载一个在作者的计算机上按照上述步骤捕获的数据包跟踪文件⁵。回答下列问题

5. 找到解析名称gai a的第一个DNS查询消息。美国的。edu. 什么DNS查询消息的跟踪中是否有包号6？此查询消息是通过UDP或TCP发送的吗？
6. 现在，请找到与初始DNS查询对应的DNS响应。什么是DNS响应消息的跟踪中的数据包号？此响应消息是否通过UDP或TCP收到？
7. DNS查询消息的目标端口是什么？源端口是什么的DNS响应消息吗？
8. DNS查询消息被发送到哪个IP地址？
9. 检查DNS查询消息。这个DNS消息有多少个“问题”包含它包含了多少个“答案”的答案？
10. 检查对初始查询消息的DNS响应消息。有多少此DNS消息是否包含“问题”？它包含了多少个“答案”的答案？
11. 基本文件http://gai a. cs. umass. edu/kurose_ross/引用的网页图像对象http://gai a. cs. umass. edu/kurose_ross/header_graphic_book_8E_2.jpg，和网页一样，是在盖亚上。美国的。edu. 基本文件http://gai a. cs. umass. edu/kurose_ross/的初始HTTP GET请求的跟踪数据包号是多少？在解析gai a. cs. umass. edu的DNS查询跟踪中的数据包号是什么，以便这个初始HTTP请求可以发送到gai a. cs. umass. edu IP地址？在接收到的DNS响应的跟踪中的数据包号是多少？对于图像对象http://gai a. cs. umass. edu/kurose_ross/header_graphic_book_8E2.jpg？的HTTP GET请求的跟踪中的数据包号是多少DNS查询中的数据包号是多少，以便这第二个HTTP请求可以发送到gai a. cs. umass. edu IP地址？讨论DNS缓存如何影响这最后一个问题的答案。

现在让我们玩一下nslookup⁷。

启动数据包捕获。

在www上做一个网络查找。美国的。edu

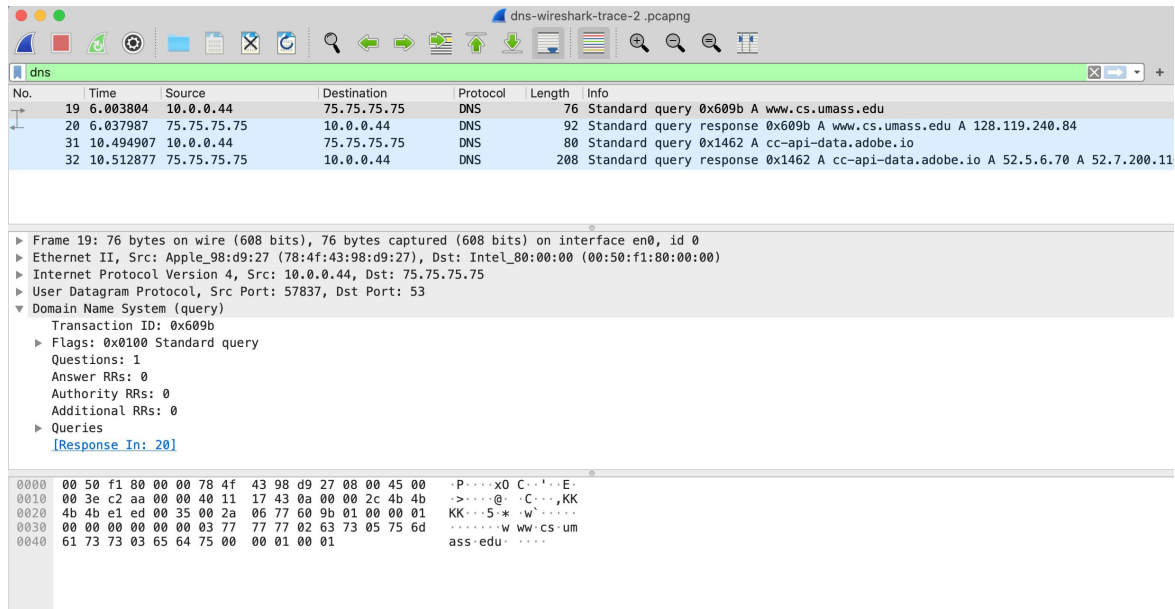
停止数据包捕获。

⁵ 您可以下载zip文件<http://gai a. cs. umass. edu/wireshark-labs/wireshark-traces-8.1.zip>并提取跟踪文件<http://gai a. cs. umass. edu/wireshark-labs/wireshark-traces-8.1.zip>-跟踪1-1。这些跟踪文件可以用来回答这些线鲨鱼实验室的问题，而不需要自己捕获数据包。每个跟踪都是使用在作者的计算机上运行的线鲨鱼进行的，同时执行线鲨鱼实验室中指示的步骤。下载了跟踪文件后，您可以将其加载到Wireshark中，并使用文件下拉菜单查看跟踪，选择打开，然后选择跟踪文件名。

⁶ 记住，这个“包号”是由Wireshark指定的列出目的；它不是包含在任何真实包头中的包号。

⁷ 如果您无法运行有线鲨鱼和捕获跟踪文件，或者正在使用LMS，请使用上面脚注中的跟踪文件dn快速鲨鱼-跟踪-2来回答下面的问题12-16。

你应该在你的线鲨窗口中得到一个类似于下面的痕迹。
让我们看看第一种类型A查询(下图是包号19,并由该包的信息列中的“A”表示)。



12. DNS查询消息的目标端口是什么?源端口是什么的DNS响应消息?
13. DNS查询消息被发送到哪个IP地址?这是你的IP地址吗默认本地DNS服务器?
14. 检查DNS查询消息。DNS查询的“类型”是什么?做的查询消息包含任何“答案”吗?
15. 检查对查询消息的DNS响应消息。有多少此DNS响应消息是否包含“问题”?有多少个“答案”?

最后,让我们使用nslookup发出命令,返回类型NS DNS记录,输入以下命令:
类型=NS嗯.edu
然后回答以下问题8:

16. DNS查询消息被发送到哪个IP地址?这是你的IP地址吗默认本地DNS服务器?
17. 检查DNS查询消息。这个查询有多少个问题?查询消息是否包含任何“答案”?
18. 检查DNS响应消息。这个回答有多少个答案?答案中包含了哪些信息?新增资源多少

8 如果您无法运行有线鲨鱼和捕获跟踪文件,或者正在使用LMS,请使用上面脚注中的跟踪文件
dn快速鲨鱼-跟踪-3来回答下面的问题17-19。

是否返回记录？在这些附加的资源记录中包含了哪些附加信息？