实验二

DNS

**实验目的**

如教科书第2.4节所述，域名系统（DNS）将主机名转换为IP地址，在互联网基础设施中发挥着关键作用。在这个实验室里，我们将仔细观察DNS的客户端。回想一下，DNS中的客户机角色相对简单——客户机向其本地DNS服务器发送一个查询，然后接收一个响应。——如教科书中的图2.19和2.20所示，在DNS客户机看不见的封面下，许多内容可以继续进行，因为分层DNS服务器相互通信，或者递归地进行或者迭代地解析客户机的DNS查询。然而，从DNS客户机的角度来看，协议相当简单——向本地DNS服务器制定查询并从该服务器接收响应。

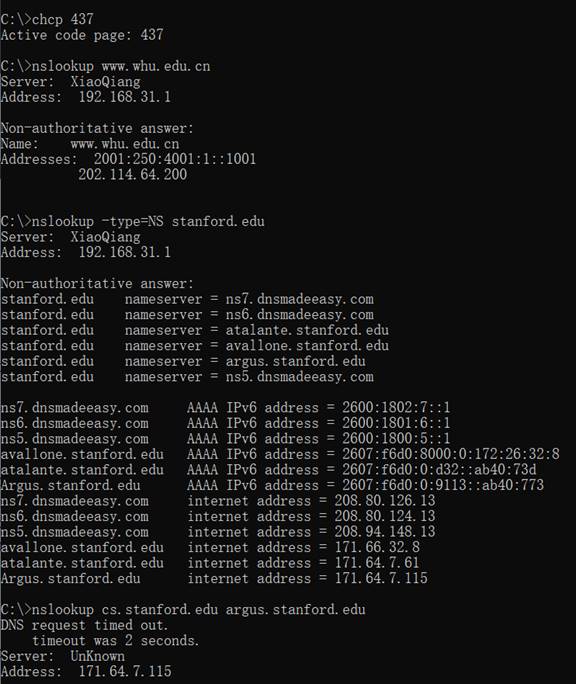
**实验步骤**

在开始这个实验之前，请先阅读教科书的2.4节来复习DNS。特别是，你可能想复习关于本地DNS服务器、DNS缓存、DNS记录和消息以及DNS记录中的TYPE字段的资料。

一、nslookup查找

在这个实验室中，我们可以广泛使用nslookup工具，它现在在大多数Linux/Unix和Microsoft平台上都可用。要在Linux/Unix中运行nslookup，只需在命令行中键入nslookup命令。要在Windows中运行它，请打开命令提示符并在命令行上运行nslookup。

在最基本的操作中，nslookup工具允许运行该工具的主机查询任何指定的DNS服务器以获取DNS记录。查询的DNS服务器可以是根DNS服务器、顶级域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）。为了完成此任务，nslookup向指定的DNS服务器发送DNS查询，从同一DNS服务器接收DNS回复，并显示结果。



上面的屏幕截图显示了几个独立命令的结果（显示在Windows命令提示符中）。第一个命令行chcp 437将Windows命令提示符的显示代码页更改为代码页437。此命令将设置终端以英文字符显示所有输入命令的结果。

除了第一行之外，接下来的所有命令都是nslookup命令。在此示例屏幕截图中，客户端主机位于武汉市的家庭网络中，其中默认的本地DNS服务器为IP地址192.168.31.1（服务器名为小强），由家庭网络的小米智能路由器配置。运行nslookup时，如果没有指定DNS服务器，那么nslookup会将查询发送到默认DNS服务器，在本例中是小强。考虑第二个命令：

nslookup www.whu.edu.cn

换句话说，这个命令是“请给我发送主机的IP地址www.whu.edu.cn”。如截图所示，此命令的响应提供两条信息：（1）提供答案的DNS服务器的名称和IP地址；（2）答案本身，即www.whu.edu.cn的主机名和IP地址。尽管响应来自本地DNS服务器，但是这个本地DNS服务器很有可能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。

现在考虑第三个命令：

nslookup –type=NS stanford.edu

在这个例子中，我们提供了选项-type=NS-和域-tanford.edu。这将导致nslookup向默认本地DNS服务器发送对NS类型记录的查询。换句话说，问题是，请把斯坦福大学权威域名系统的主机名发给我。（当不使用“类型”选项时，nslookup使用默认值，即查询类型A记录。）在上面的屏幕截图中显示的答案首先指示提供答案的DNS服务器（这是默认的本地DNS服务器）以及六个斯坦福名称服务器。这些服务器中的每一个都是斯坦福大学校园主机的权威DNS服务器，其中三个服务器使用dnsmadeeasy.com提供的动态DNS主机服务。然而，nslookup还指出答案是“on authoritive”，这意味着这个答案来自某个服务器的缓存，而不是来自权威的斯坦福DNS服务器。最后，答案还包括斯坦福大学权威DNS服务器的IP地址。（即使nslookup生成的类型NS查询没有显式地请求IP地址，本地DNS服务器还是返回了这些揻或free-，nslookup将显示结果。）

现在最后考虑第四个命令：

nslookup cs.stanford.edu argus.stanford.edu

在本例中，我们指出要将查询发送到DNS服务器argus.stanford.edu，而不是默认的DNS服务器。因此，查询和应答事务直接发生在查询主机和argus.stanford.edu之间。在本例中，DNS服务器argus.stanford.edu提供主机cs.stanford.edu的IP地址。

现在我们已经介绍了几个示例，您可能想知道nslookup命令的一般语法。语法为：

nslookup –option1 –option2 host-to-find dns-server

通常，nslookup可以使用0、1、2或更多选项运行。正如我们在上面的例子中看到的，dns服务器也是可选的；如果没有提供，查询将被发送到默认的本地dns服务器。

现在我们已经提供了nslookup的概述，现在是您自己测试它的时候了。执行以下操作（并记录结果）：

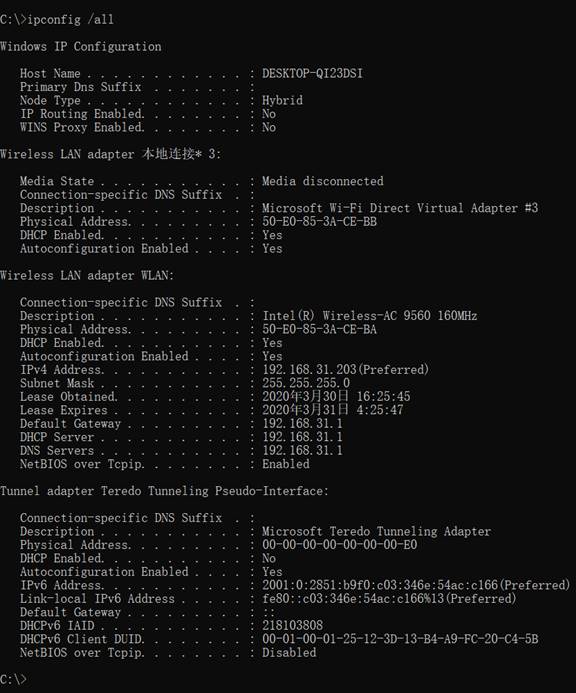
1. 运行nslookup获取中国Web服务器的IP地址。那台服务器的IP地址是多少？
2. 运行nslookup来确定欧洲某大学的权威DNS服务器。
3. 运行nslookup，以便查询问题2中获得的其中一个DNS服务器以获得Yahoo！的邮件服务器！邮件。牋它的IP地址是什么？

2、ipconfig配置

*ipconfig配置*（对于Windows）和ifconfig（对于Linux/Unix）是主机中最有用的小实用程序，特别是对于调试网络问题。这里我们只描述ipconfig，尽管Linux/Unix ifconfig非常相似。ipconfig可用于显示当前的TCP/IP信息，包括您的地址、DNS服务器地址、适配器类型等。例如，如果您只需输入

ipconfig /all

进入命令提示符，如下面的屏幕截图所示。



*ipconfig配置*对于管理存储在主机中的DNS信息也非常有用。在第2.5节中，我们了解到主机可以缓存它最近获得的DNS记录。要查看这些缓存记录，请在提示C:\>后提供以下命令：

ipconfig /displaydns

每个条目以秒为单位显示剩余生存时间（TTL）。要清除缓存，请输入

ipconfig /flushdns

刷新DNS缓存将清除所有条目并从主机文件重新加载条目。

三、用Wireshark跟踪DNS

既然我们已经熟悉了nslookup和ipconfig，我们就可以着手做一些严肃的工作了。让抯首先捕获由普通网络冲浪活动生成的DNS包。

使用清空主机中的缓存。

打开你的浏览器，清空你的浏览器缓存。

打开，在过滤器中输入搃庠，然后用获取你的搃庠。此筛选器将删除所有既不是源数据包也不是目的地数据包。

从开始抓包。

使用浏览器访问网页：

停止抓包。

回答下列问题。只要有可能，当你回答下面的问题时，你应该在你用来回答问题的轨迹中交一份打印出来的数据包。要打印数据包，请使用“文件”->“打印”，选择“仅选定数据包”，选择“数据包摘要行”，然后选择回答问题所需的最小数据包详细信息量。

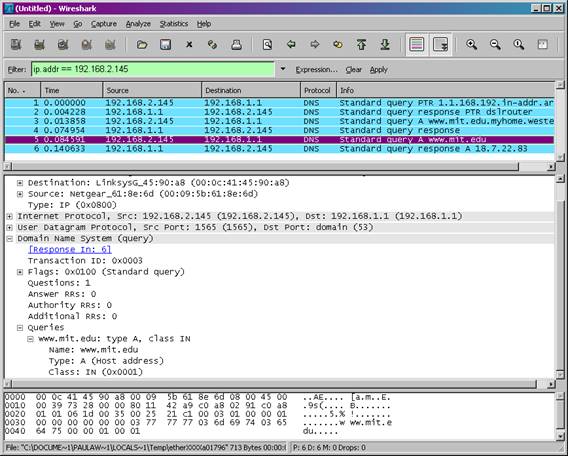
1. 找到DNS查询和响应消息。它们是通过UDP还是TCP发送的？
2. DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？
3. DNS查询消息发送到哪个IP地址？使用ipconfig确定本地DNS服务器的IP地址。这两个IP地址相同吗？
4. 检查DNS查询消息。DNS查询的类型是什么？查询消息是否包含任何应答器？
5. 检查DNS响应消息。提供了多少答案？这些答案都包含什么？
6. 考虑主机发送的后续TCP SYN数据包。SYN包的目标IP地址是否对应于DNS响应消息中提供的任何IP地址？
7. 此网页包含图像。在检索每个映像之前，主机是否发出新的DNS查询？

现在让我们来玩nslookup。

启动包捕获。

在上做一个

停止抓包。

你应该得到如下的痕迹： **

我们从上面的截图中看到，nslookup实际上发送了三个DNS查询并收到了三个DNS响应。在本作业中，在回答以下问题时，请忽略前两组查询/响应，因为它们是nslookup特有的，通常不是由标准Internet应用程序生成的。相反，您应该关注最后的查询和响应消息。

DNS查询消息的目标端口是什么？DNS响应消息的源端口是什么？DNS查询消息发送到哪个IP地址？这是默认本地DNS服务器的IP地址吗？检查DNS查询消息。DNS查询的类型是什么？查询消息是否包含任何应答器？检查DNS响应消息。提供了多少答案？这些答案都包含什么？提供屏幕截图。

现在重复上一个实验，但是发出命令：

nslookup –type=NS stanford.edu

回答下列问题：

1. DNS查询消息发送到哪个IP地址？这是默认本地DNS服务器的IP地址吗？
2. 检查DNS查询消息。DNS查询的类型是什么？查询消息是否包含任何应答器？
3. 检查DNS响应消息。响应消息提供了什么斯坦福名称服务器？此响应消息是否还提供了斯坦福命名者的IP地址？
4. 提供屏幕截图。

现在重复上一个实验，但是发出命令：

nslookup cs.stanford.edu argus.stanford.edu

回答下列问题：

1. DNS查询消息发送到哪个IP地址？这是默认本地DNS服务器的IP地址吗？如果不是，IP地址对应什么？
2. 检查DNS查询消息。DNS查询的类型是什么？查询消息是否包含任何应答器？
3. 检查DNS响应消息。提供了多少答案？这些答案都包含什么？
4. 提供屏幕截图。

[[一]](" \l "_ftnref1" \o ")我们所说的“不通知”是什么意思？在你的实验报告中，请突出显示你在打印输出中找到答案的地方，并添加一些文字（最好是用彩色框），注明你在突出显示和注释中发现的内容。