**实验报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **学　　号** |  | **姓　　名** |  | **专业、班** |  |

# 实验5利用Ethereal分析HTTP和DNS

一、 实验目的及任务

* 熟悉并掌握Ethereal的基本操作，了解网络协议实体间的交互以及报文交换。
* 分析HTTP协议
* 分析DNS协议

二、 实验设备

与因特网连接的计算机网络系统；主机操作系统为Windows2000或Windows XP；Ethereal等软件。

三、 实验步骤

(一) HTTP分析

1、捕获HTTP分组

* 在进行跟踪之前，为了确保web网页是从网络中获取而不是从高速缓冲中取得的，我们首先清空 Web 浏览器的高速缓存。之后，还要在客户端清空 DNS 高速缓存，来确保web服务器域名到IP地址的映射是从网络中请求的。在winxp机器上，可在命令提示行输入：ipconfig /flushdns
* 启动Ethereal,开始捕获
* 在web浏览器输入：www.google.cn
* 停止分组捕获。

根据捕获窗口内容，回答下列问题。

* 1. 被访问服务器的IP地址是多少？
  2. 用户访问服务器的过程中使用了哪些协议？

2、HTTP GET/response交互

* 首先通过下载一个非常简单的HTML文件（该文件非常短，并且不嵌入任何对象）。
* 启动Web 浏览器，然后启动Ethereal。在窗口的显示过滤规则编辑框处输入“http”，分组列表子窗口中将只显示所捕获到的HTTP消息。
* 设置好以后，开始Ethereal分组捕获。
* 在打开的Web浏览器窗口中输入以下地址（浏览器中将显示只有两行文字的、非常简单的一个HTML文件）：
* <http://gaia.cs.umass.edu/search.html>
* 停止分组捕获。

根据捕获窗口内容，回答下列问题。

* 1. 你的浏览器使用的是HTTP1.0，还是HTTP1.1？你所访问的Web服务器所使用HTTP协议的版本号是多少？
  2. 你的浏览器向服务器指出它能接收何种语言版本的对象？
  3. 你的计算机的IP地址是多少？服务器gaia.cs.umass.edu的IP地址是多少？
  4. 从服务器向你的浏览器返回response消息的状态代码是多少？
  5. 你从服务器上所获取的HTML文件的最后修改时间是多少？
  6. 返回到浏览器的内容一共多少字节？

3、HTTP 条件GET/response交互

* + - 启动浏览器，清空浏览器的缓存（在浏览器中，选择“工具”菜单中的“Internet选项”命令，在出现的对话框中，选择“删除文件”）。
    - 启动Ethereal。开始Ethereal分组捕获。
    - 在浏览器的地址栏中输入以下URL: <http://gaia.cs.umass.edu/search.html>
    - 在你的浏览器中重新输入相同的URL或单击浏览器中的“刷新”按钮。
    - 停止Ethereal分组捕获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所捕获到的HTTP消息。

根据操作回答下列问题。

* + - 1. 分析你的浏览器向服务器发出的第一个HTTP GET请求的内容，在该请求消息中，是否有一行是：IF-MODIFIED-SINCE？
      2. 分析服务器响应消息的内容，服务器是否明确返回了文件的内容？如何获知？
      3. 分析你的浏览器向服务器发出的第二个“HTTP GET”请求，在该请求报文中是否有一行是：IF-MODIFIED-SINCE？如果有，在该首部行后面跟着的信息是什么？
      4. 服务器对第二个HTTP GET请求的响应消息中，服务器是否明确返回了文件的内容？请解释。

4、获取长文件

* + - * + 启动浏览器，将浏览器的缓存清空。
        + 启动Ethereal，开始Ethereal分组捕获。
        + 在浏览器的地址栏中输入以下URL: <http://www10.zzu.edu.cn/hgyl/wlkt/html/index1.htm>
        + 浏览器将显示一个长的文本。
        + 停止Ethereal分组捕获，在显示过滤筛选编辑框中输入“http”,分组列表子窗口中将只显示所捕获到的HTTP消息。

根据操作回答回答下列问题。

你的浏览器一共发出了多少个HTTP GET请求？

承载这一个HTTP响应报文一共需要多少个TCP报文段？

5、嵌有对象的HTML文档

启动浏览器，将浏览器的缓存清空。

启动Ethereal。开始Ethereal分组捕获。

在浏览器的地址栏中输入以下URL: <http://www.scut.edu.cn/english/index.html>

浏览器将显示一个包含两个图片的短HTTP文件

停止Ethereal分组捕获，在显示过滤筛选说明处输入“http”,分组列表子窗口中将只显示所捕获到的HTTP消息。

根据操作回答下列问题。

你的浏览器一共发出了多少个HTTP GET请求消息？这些请求消息被发送到的目的地IP地址是多少？

（二）DNS 分析

nslookup工具允许主机向指定的DNS服务器查询某个DNS记录。如果没有指明DNS服务器，nslookup将把查询请求发向默认的DNS服务器。

nslookup的一般格式是：

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

ipconfig命令用来显示你当前的TCP/IP信息，包括：你的地址、DNS服务器的地址、适配器的类型等信息。如果，要显示与主机相关的信息用命令：

ipconfig/all

如果查看DNS缓存中的记录用命令：

ipconfig/displaydns

要清空DNS缓存，用命令：

ipconfig /flushdns

（注：这时候可能就会出现标题上的错误提示：

C:\Documents and Settings\Administrator>ipconfig /flushdns

Windows IP Configuration

Could not flush the DNS Resolver Cache: 执行期间，函数出了问题。

如果遇到这个提示的错误，可以打开dns client 和 dhcp client 两个服务尝试一下。

执行：控制面板--管理工具--服务 中把DNS Client和DHCP client两个服务组件启动。

如果禁用了两个服务，可以设置手动或自动，然后点启动，再运行完 ipconfig /flushdns 命令后，如果可以再禁用。）

运行以上命令需要进入MSDOS环境。(开始菜单－>运行－>输入命令“cmd”)

1、跟踪DNS（1）

* 利用ipconfig命令清空主机上的DNS缓存。启动浏览器，并将浏览器的缓存清空。
* 启动Ethereal，在显示过滤筛选规则编辑框处输入： “ip.addr = = your\_IP\_address”(如：ip.addr= =10.17.7.23)
* 过滤器将会删除所有目的地址和源地址与指定IP地址都不同的分组。
* 开始Ethereal分组捕获。
* 在浏览器的地址栏中输入：<http://www.ietf.org>
* 停止分组捕获。

根据操作回答下列问题。

* 1. 定位到DNS查询消息和查询响应报文，这两种报文的发送是基于UDP还是基于TCP的？
  2. DNS查询消息的目的端口号是多少？DNS查询响应消息的源端口号是多少？
  3. DNS查询消息发送的目的地的IP地址是多少？利用ipconfig命令（ipconfig /all）查看你主机的本地DNS服务器的IP地址。这两个地址相同吗？
  4. 检查DNS查询消息，该查询报文中包含“answers”吗？
  5. 检查DNS查询响应消息，其中共提供了多少个“answers”？每个answers包含哪些内容？
  6. 打开的WEB页中包含图片，在获取每一个图片之前，你的主机发出新的DNS查询了吗？

2、跟踪DNS（2）

* + - 开始Ethereal分组捕获。
    - 在www.mit.edu上进行nslookup（即执行命令：nslookup www.mit.edu）。
    - 停止分组捕获。

根据操作回答下列问题。

* + - 1. DNS查询消息的目的端口号是多少？DNS查询响应消息的源端口号是多少？
      2. DNS查询消息发送的目的地的IP地址是多少？这个地址是你的默认本地DNS服务器的地址吗？
      3. 检查DNS查询消息，该查询消息中包含“answers”吗？
      4. 检查DNS查询响应消息，其中提供了多少个“answers”？每个answers包含哪些内容？

3、跟踪DNS（3）

* + - * + 重复上面的实验，只是将命令替换为：nslookup –type=NS mit.edu

根据操作回答下列问题。

DNS查询消息发送的目的地的IP地址是多少？这个地址是你的默认本地DNS服务器的地址吗？

检查DNS查询消息，该查询报文中包含“answers”吗？

检查DNS查询响应消息，其中响应消息提供了哪些MIT名称服务器？响应消息提供这些MIT名称服务器的IP地址了吗？

4、跟踪DNS（4）

重复上面的实验，只是将命令替换为：nslookup [www.aiit.or.kr](http://www.aiit.or.kr) bitsy.mit.edu

根据操作回答下列问题。

DNS查询消息发送的目的地的IP地址是多少？这个地址是你的默认本地DNS服务器的地址吗？如果不是，这个IP地址相当于什么？

检查DNS查询消息，它是哪一类型的DNS查询？该查询报文中包含“answers”吗？

检查DNS查询响应消息，其中提供了多少个“answers”？每个answers包含哪些内容？