实验1　网络的使用与配置

§ 1.1 实验目的

熟悉 TCP/IP 通信原理，熟练地掌握典型的 TCP/IP 应用程序的使用与设置，熟悉 Linux 下抓包工具 tcpdump 的使用。

§ 1.2 预备知识

TCP/IP 通信的基本概念：IP 地址、IP 端口、子网屏蔽、IP 子网、路由器等。TCP/IP 应用协议族的内容和功能：DNS 名字/地址解析协议、ARP 协议、FTP 协议、HTTP 协议和 SMTP 协议。

§ 1.3 实验内容

§1.3.1 wget 下载命令使用

1. 学习“wget”的各种使用方法，完成以下功能并在实验报告中记录所使用的命令。（关于如何使用 wget 请参看附录：“wget 使用”或使用 man wget 查看帮助）
   - 断点续传
   - 后台运行下载任务
   - 利用编写下载 URL 列表文件的方法实现下载批量文件
   - 下载指定后缀名的文件（需要与-m 或者-r 等参数结合使用）（创建目录结构和不创建目录结构两种情况）
   - 下载除某后缀名之外的文件（需要与-m 或者-r 等参数结合使用）（创建目录结构和不创建目录结构两种情况）
   - 下载某网站上一个完整的子目录（镜像）eg: ftp://debian.ustc.edu.cn/debian/tools/
2. 在实验报告中解释下列命令行的含义：
   - wget -r -nH ftp://10.1.1.1/movie/
   - wget -r -R "*.htm*\?*" -k http://www.abc.com/blog
   - wget -r -k http://www.abc.com/blog
   - wget -r -l2 -k http://www.abc.com/blog
   - wget -nc -r -k http://www.abc.org/help/
   - wget -i your.file

§1.3.2 熟悉抓包工具 tcpdump

tcpdump 可以将网络中传送的数据包的“头”完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤，并提供 and、or、not 等逻辑语句来帮助你去掉无用的信息。tcpdump 就是一种免费的网络分析工具，尤其其提供了源代码，公开了接口，因此具备很强的可 扩展性，对于网络维护和入侵者都是非常有用的工具。

tcpdump 的命令格式为：

tcpdump [-adeflnNOpqStvx] [-c 数量] [-F 文件名] [-i 网络接口]
[-r 文件名] [-s snaplen] [-T 类型] [-w 文件名] [表达式]

tcpdump 利用表达式作为过滤报文的条件，如果一个报文满足表达式的条件，则这个报文将会被捕获。如果没有给出任何条件，则网络上所有的信息包将会 被截获。

表达式中需要注意的关键字：

1、关于类型的关键字，主要包括 host、net、port。例如 host 202.38.75.11，指明 202.38.75.11 是一台主机，net 202.38.0.0 指明 202.38.0.0 是一个网络地址，port 23 指明端口号是 23。

2、确定传输方向的关键字，主要包括 src、dst、dst or src、dst and src，这些关键字指明了传输的方向。例如 src 202.38.75.11 指明 ip 包中源地址是 202.38.75.11，dst net 202.38.0.0 指明目的网络地址是 202.38.0.0。

这些关键字可以组合起来构成强大的组合条件来满足人们的需要，例如 tcpdump host 202.38.75.11 and port 80

本实验要求熟悉 tcpdump 的使用，用 man tcpdump 查看帮助

§1.3.3 观察 FTP 的两种数据传送模式：

本实验在 Linux 环境下实现，使用 tcpdump 观察 FTP 的两种数据传输模式（主动模式和被动模式）的区别，在观察被动模式时请注意观察 FTP 命令：PASV 命令；在观察主动模式时请注意观察 FTP 命令：PORT 命令。

记录主动模式和被动模式的关键数据，并在实验报告中进行分析。

说明：

1. Linux 下命令行模式下的 ftp 客户端程序是 ftp,可以在 ftp 客户端里输入 passive 命令在主动模式和被动模式之间切换。
2. 如果使用 lftp 客户端，可以输入 set ftp:passive-mode off 关闭被动模式。
3. 如果在图形界面下，同学们也可以使用图形化界面的 gftp 客户端工具，通过对选项的设置可以实现主动模式和被动模式的切换。
4. 请同学们自己设计 tcpdump 的命令格式（注意使用-X 选项），并且使用上述 ftp 客户端程序连接某 ftp 服务器（推荐 202.38.64.123、debian.ustc.edu.cn 或 mail.ustc.edu.cn，大家可以自己随意选取），然后分析 tcpdump 抓到的数据包，对比 ftp 主动模式和被动模式的区别。

§1.3.4 了解 DNS 域名服务

熟悉使用 nslookup 查找 DNS 服务器上登记的域名，记录几次查询的结果，及服务器的 ip。使用 nslookup 查找名字服务器上登记的域名。分别使用 202.38.64.1 和 202.38.75.11 作为名字服务器进行查找。分别记录以下结果：

1. 某个子域下的一部分主机的名字－IP 地址对应关系，如 flame.nsrl.ustc.edu.cn—202.38.77.223；
2. 通过 IP 地址查找主机名，即：反向查询，记录你的查询结果；
3. 指定使用 202.38.75.11 作为 DNS 服务器，重复 2、3；
4. 查看当前的查询选项（set all）
5. 查询邮件交换记录 MX（如 mail.ustc.edu.cn）
6. 查询某个域的域名服务器（如 ustc.edu.cn 的域名服务器）

以上记录数目不限，多少均可，但尽量不要和别人的完全重复。

§ 1.4 实验报告要求

1. 完成实验内容中要求记录的部分。
2. 完成实验内容中要求记录部分的分析。
3. 说明在实验过程中遇到的问题和解决方法。
4. ftp 协议在客户端和服务器之间使用了几个 TCP 连接？这样做有何优点？“被动（passive）”方式是如何工作的？请用实验中记录的现象加以说明。
5. 简要说明 tcpdump 的作用，在实验中用到了那些参数和表达式的关键字，说明这些参数和表达式的作用。
6. DNS 服务器的功能是什么？人们为什么要使用它们？Internet 上的 DNS 服务器结构是怎么样的？*它们之间如何保持名字/地址数据的一致性？
7. 请列举一些常用的下载工具及其软件编写公司或个人，这些软件各有什么优缺点。