实验一 参考文档

wget 工具使用

wget 是一个命令行工具，用于批量下载文件，支持 HTTP 和 FTP。wget 基本上所有的 Linux 版本都自己带了，Windows 下面的用户可以使用 wget 的 win32 的版本，基本功能完全一致。下载地址 http://www.gnu.org/software/wget/。注意：因为 wget 是命令行程序没有图形界面，Windows 下运行 wget 的时候在 DOS Shell 中运行。

wget 的基本用法

wget 的基本使用形式是“wget [参数列表] URL”。下表中列出了常用的参数及其含义，请在实验过程中对这些参数的设置进行练习。

参数	参数含义
--help	显示 wget 的联机帮助，本表中仅仅给出了部分参数的使用，更详细的参数使用请查阅联机帮助
-A	表示仅接受指定的文件类型，如-A "*.gif"将仅下载 gif 图片，如果有多个允许可以使用“,”分开
-b	让 wget 在后台运行，记录文件写在当前目录下"wget-log"文件中
-t [nuber of times]	当 wget 无法与服务器建立连接时，尝试连接多少次。比如"-t 120"表示尝试 120 次。当这一项为"0"的时候，指定尝试无穷多次直到连接成功为止
-c	断点续传，这也是个非常有用的设置，特别当下载比较大的文件的时候，如果中途意外中断，那么连接恢复的时候会从上次没传完的地方接着传，而不是又从头开始
-T [number of sec]	超时时间。如"-T 120"表示如 120 秒以后远程服务器没有发过来数据，就重新尝试连接。如果网络速度比较快，这个时间可以设置的短些
-w [number of seco]	在两次尝试之间等待多少秒，比如"-w 100"表示两次尝试之间等待 100 秒
-Q [byetes]	限制下载文件的总大小不能超过多少，如"-Q2k"表示不能超过 2K 字节，"-Q3m"表示不能超过 3M 字节
-nd	不下载目录结构，把从服务器所有指定目录下载的文件都堆到当前目录里
-x	与"-nd"设置刚好相反，如"wget -x http://a.b.c"将创建在当前目录下创建"a.b.c"子目录，然后按照服务器目录结构一级一级建下去，直到所有的文件都传完
-nH	不创建以目标主机域名为目录名的目录，将目标主机的目录结构直接下到当前目录下
--http-user=xxx	如果 Web 服务器需要指定用户名和口令，用这两项来设定
--http-passwd=xxx	
-i download_list	下载文件“download_list”中列出的所有 URL

-k	将链接转换为本地连接
--proxy-user=xxx	如果代理服务器需要输入用户名和口令，使用这两个选项
--proxy-passwd=xxx	
-r	--recursive specify recursive download
-R	指定拒绝的文件类型，如-R "*.gif"将不下载 gif 图片，如果有多个不允许，可以使用“,”分开
-l [depth]	下载远程服务器目录结构的深度，例如"-l 5"下载目录深度小于或者等于 5 以内的目录结构或者文件
-m	做站点镜像时的选项，如果你想做一个站点的镜像
-np	只下载目标站点指定目录及其子目录的内容

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

另外可参考：

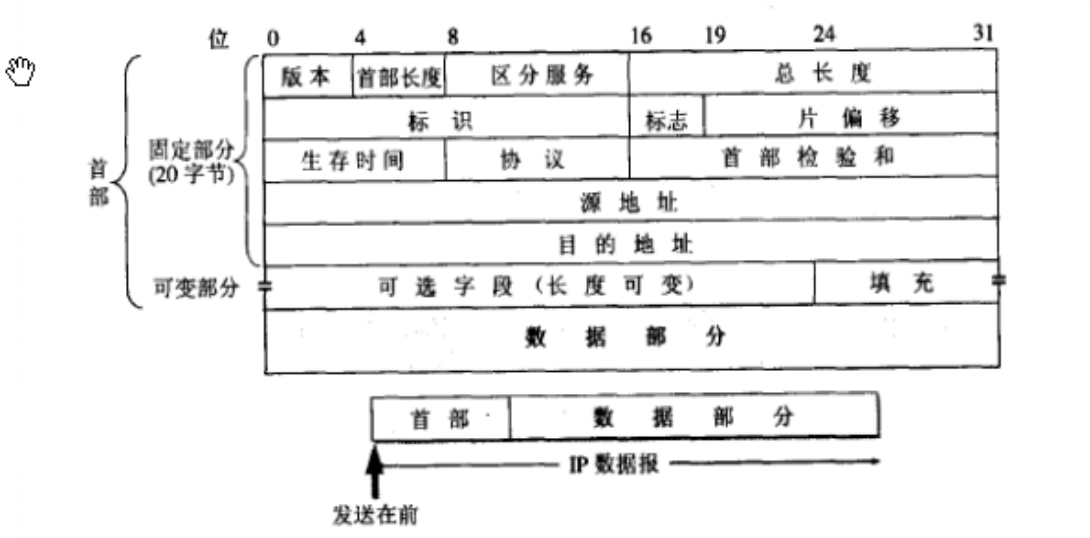
http://abing9.blog.51cto.com/842474/660872

http://www.cnblogs.com/ggjucheng/archive/2012/01/14/2322659.html

帧格式说明

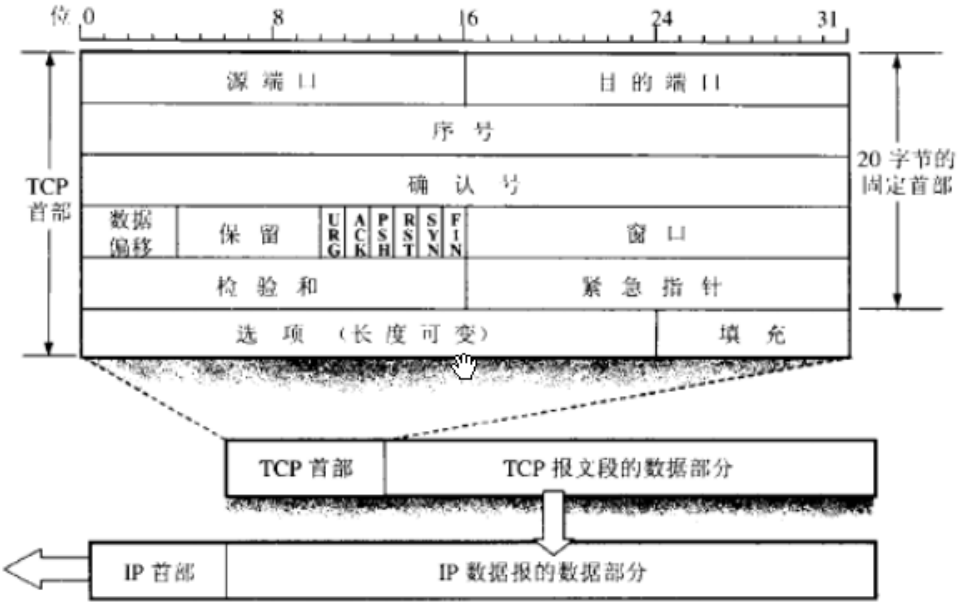
1. IP 帧格式：

IP 帧格式



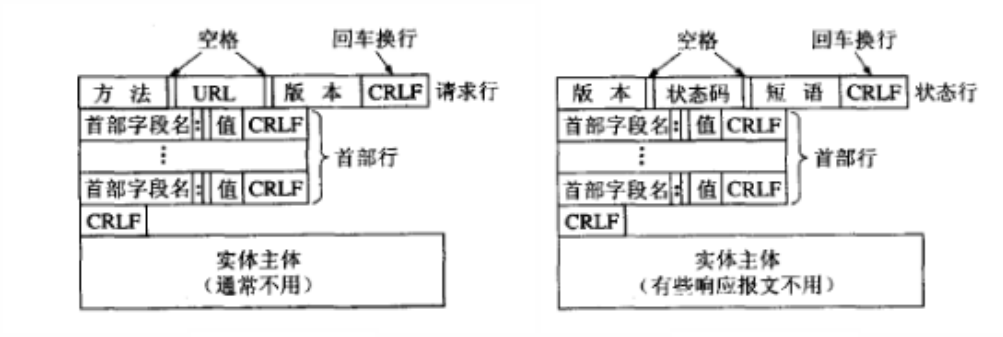
2. TCP 帧格式：

TCP 帧格式



3. HTTP 帧格式：

HTTP 帧格式



请求报文　　响应报文

开始行：区分请求报文还是响应报文

首部行：说明浏览器、服务器或是报文主体的一些信息

请求行：方法（命令）、请求资源的 URL、HTTP 的版本

方法（操作）	意义
OPTION	请求一些选项的信息
GET	请求读取由 URL所标志的信息
HEAD	请求读取由 URL所标志的信息的首部
POST	给服务器添加信息（例如，注释）
PUT	在指明的 URL下存储一个文档
DELETE	删除指明的 URL所标志的资源
TRACE	用来进行环回测试的请求报文
CONNECT	用于代理服务器

状态行：HTTP 的版本、状态码、解释状态码的简单短语。

状态码：3 位，分为 5 大类 33 种

1xx 表示通知信息的，如请求收到了或正在进行处理。

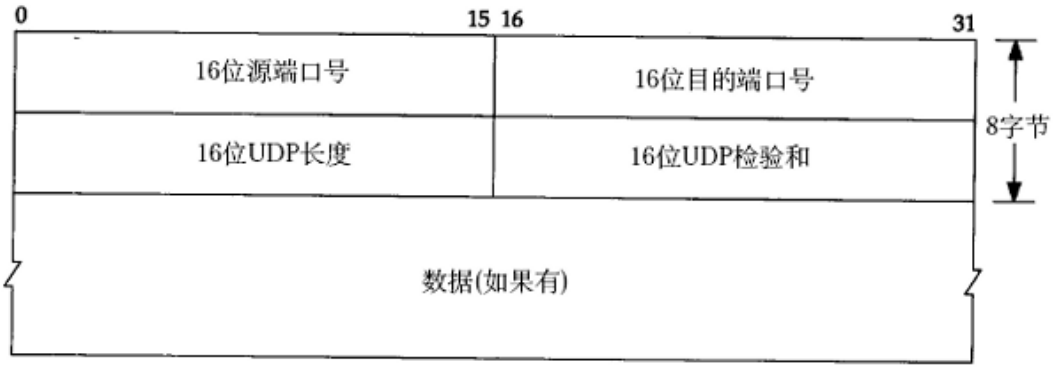
2xx 表示成功，如接受或知道了。

3xx 表示重定向，表示要完成请求还必须采取进一步的行动。

4xx 表示客户的差错，如请求中有错误的语法或不能完成。

5xx 表示服务器的差错，如服务器失效无法完成请求。

4. UDP 帧格式



Linux 下 nslookup 常用交互式命令

>server *domain*

>lserver *domain*　　改变查询服务器为 *server*

>set *keyword*[=*value*]　　按指定方式查询

all

Prints the current values of the frequently-used options to **set** Information about the current default server and host is also printed.

class= *value*

Change the query class to one of:

IN

the Internet class

CHAOS

the Chaos class

HESIOD

the MIT Athena Hesiod class

ANY

wildcard (any of the above)

The class specifies the protocol group of the information.

(Default = **IN** ; abbreviation = **cl**

querytype= *value*

type= *value*

Change the type of information query to one of:

A

the host's Internet address.

CNAME

the canonical name for an alias.

HINFO

the host CPU and operating system type.

MINFO

the mailbox or mail list information.

MX

the mail exchanger.

NS

the name server for the named zone.

PTR

the host name if the query is an Internet address; otherwise, the pointer to other information.

SOA

the domain's ``start-of-authority '' information.

TXT

the text information.

UINFO

the user information.

WKS

the supported well-known services.

Other types (**ANY**, **AXFR**, **MB**, **MD**, **MF**, **NULL**) are described in the RFC-1035 document.

(Default = A)

A 地址记录(Ipv4)

AAAA 地址记录（Ipv6）
AFSDB Andrew 文件系统数据库服务器记录（不懂）
ATMA ATM 地址记录（不是自动提款机）
CNAME 别名记录
HINFO 硬件配置记录，包括 CPU、操作系统信息
ISDN 域名对应的 ISDN 号码
MB 存放指定邮箱的服务器
MG 邮件组记录
MINFO 邮件组和邮箱的信息记录
MR 改名的邮箱记录
MX 邮件服务器记录
NS 名字服务器记录
PTR 反向记录（从 IP 地址解释域名）
RP 负责人记录
RT 路由穿透记录（不懂）
SRV TCP 服务器信息记录（将有大用处）
TXT 域名对应的文本信息
X25 域名对应的 X.25 地址记录

Windows 下 nslookup 使用

$ nslookup HOSTNAME
查 HOSTNAME 对应的 IP 地址；
$ nslookup IP_ADDRESS
查 IP 地址对应的主机名；
$ nslookup - DNS_SERVER_IP(202.38.64.1, 202.38.75.11)
使用指定的 DNS 服务器进行查询。
nslookup 状态下:
> HOSTNAME<CR>
查 HOSTNAME 对应的 IP 地址；
> IP_ADDRESS<CR>
查 IP 地址对应的主机名；
> ls DOMAIN_NAME<CR>
给出域 DOMAIN_NAME 下的所有主机和子域的列表；
> exit
退出 nslookup。
>help
调出帮助文件：
Commands: (identifiers are shown in uppercase, [] means optional)
NAME - print info about the host/domain NAME using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ? - print info on common commands
set OPTION - set an option

```
        all                     - print options, current server and host
        [no]debug               - print debugging information
        [no]d2                  - print exhaustive debugging information
        [no]defname             - append domain name to each query
        [no]recurse             - ask for recursive answer to query
        [no]search              - use domain search list
        [no]vc                  - always use a virtual circuit
        domain=NAME             - set default domain name to NAME
        srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
        root=NAME               - set root server to NAME
        retry=X                 - set number of retries to X
        timeout=X               - set initial time-out interval to X seconds
        type=X                  - set query type (ex. A,ANY,CNAME,MX,NS,PTR,SOA,SRV)
        querytype=X             - same as type
        class=X                 - set query class (ex. IN (Internet), ANY)
        [no]msxfr               - use MS fast zone transfer
        ixfrver=X               - current version to use in IXFR transfer request
server NAME         - set default server to NAME, using current default server
lserver NAME        - set default server to NAME, using initial server
finger [USER]       - finger the optional NAME at the current default host
root                - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
        -a          -   list canonical names and aliases
        -d          -   list all records
        -t TYPE     -   list records of the given type (e.g. A,CNAME,MX,NS,PTR etc.)
view FILE           - sort an 'ls' output file and view it with pg
exit                - exit the program
```