## 1文件和目录管理

**Strings命令:** 在对象文件或二进制文件中查找可打印的字符串

Strings filename 查看文件

选项-a,查看文件全部

选项-f, 在显示字符串前先显示文件名(默认没有)

**rsync命令:**是一个远程数据同步工具，可通过LAN/WAN快速同步多台主机间的文件。rsync使用所谓的“rsync算法”来使本地和远程两个主机之间的文件达到同步，这个算法只传送两个文件的不同部分，而不是每次都整份传送，因此速度相当快。

rsync [xx] SRC DEST

rsync [xx] SRC [USER@]host:DEST

rsync [xx] [USER@]HOST:SRC DEST

rsync [xx] [USER@]HOST::SRC DEST

rsync [xx] SRC [USER@]HOST::DEST

rsync [xx] rsync://[USER@]HOST[:PORT]/SRC [DEST]

1.拷贝本地文件。当SRC和DES路径信息都不包含有单个冒号":"分隔符时就启动这种工作模式。如：rsync -a /data /backup

2.使用一个远程shell程序(rsh、ssh)来实现将本地机器的内容拷贝到远程机器。当DST路径地址包含单个冒号":"分隔符时启动该模式。

如：rsync -avz \*.c foo:src

3.使用一个远程shell程序(如rsh、ssh)来实现将远程机器的内容拷贝到本地机器。当SRC地址路径包含单个冒号":"分隔符时启动该模式。

如：rsync -avz foo:src/bar /data

4.从远程rsync服务器中拷贝文件到本地机。当SRC路径信息包含"::"分隔符时启动该模式。

如：rsync -av root@192.168.78.192::www /databack

5.从本地机器拷贝文件到远程rsync服务器中。当DST路径信息包含"::"分隔符时启动该模式。

rsync -av /databack root@192.168.78.192::www

6.远程机的文件列表。这类似于rsync传输，不过只要在命令中省略掉本地机信息即可。如：rsync -v rsync://192.168.78.192/www

选项-v, --verbose 详细模式输出

选项-q, --quiet 精简输出模式。

选项-a, 归档模式，表示以递归方式传输文件，并保持所有文件属性，

选项-r, 对子目录以递归模式处理。

选项-b, 创建备份，也就是对于目的已经存在有同样的文件名时，将老的文件重新命名为~filename。可以使用--suffix选项来指定不同的备份文件前缀。

--backup-dir 将备份文件(如~filename)存放在在目录下。

-suffix=SUFFIX 定义备份文件前缀。

选项-u, --update 仅仅进行更新，也就是跳过所有已经存在于DST，并且文件时间晚于要备份的文件，不覆盖更新的文件。

选项-p, --perms 保持文件权限。

选项-o, --owner 保持文件属主信息。

选项-g, --group 保持文件属组信息。

选项-z, --compress 对备份的文件在传输时进行压缩处理。

**du命令:** 查看文件或目录所占用的磁盘空间的大小

du [xx] Dir

-h：以人类可读的方式显示

　　 -a：显示目录占用的磁盘空间大小,还要显示其下目录和文件占用磁盘空

间的大小

　 　-s：显示目录占用的磁盘空间大小,不要显示其下子目录和文件占用的磁

盘空间大小

　　 -c：显示几个目录或文件占用的磁盘空间大小，还要统计它们的总和

　　 -l ：统计硬链接占用磁盘空间的大小

　 　-L：统计符号链接所指向的文件占用的磁盘空间大小

--max-depth=n显示最大目录深度(常常n为1)

**echo命令:** 用于在shell中打印shell变量的值，或者直接输出指定的字符串.

echo [xx] 变量

选项-e激活转义字符

\b 删除前一个字符(行中间)

\c 最后不加上换行符号(行末尾)

\f 换行但光标仍旧停留在原来的位置；

\n 换行且光标移至行首；

\r 光标移至行首，但不换行；

\t 插入tab；

\\ 插入\字符；

**颜色设置：**

**\e[1;xxm**  xx代表颜色码,在行首设置文字颜色

**\e[0m** 在行末尾，恢复原来的文字颜色

**xx: 黑色=30 红色=31 绿色=32 黄色=33 蓝=34**

**find命令：**用来在指定目录下查找文件。任何位于参数之前的字符串都将被视为欲查找的目录名。如果使用该命令时，不设置任何参数，则find命令将在当前目录下查找子目录与文件。并且将查找到的子目录和文件全部进行显示。

find startDir [xx]

选项-name<范本样式>:指定字符串作为寻找文件或目录的范本样式；

选项-links<连接数目>：查找符合指定的硬连接数目的文件或目录；

选项-perm<权限> 按照文件权限来查找文件。

选项-print 打印

选项-user<用户名>根据用户查找文件

选项-group<组名>根据组查找文件

选项-size<+/-num>查找大于或小于num的文件

选项-inum<inode>：查找符合指定的inode编号的文件或目录

选项-exec find命令对匹配的文件执行该参数所给出的其他

linux命令。***形式为 ' -exec 命令 {} \;' 注意***

***{}和 \;之间的空格,其中{}代表符合的文件。***

**install命令:**作用是安装或升级软件或备份数据，它的使用权限是所有用户。install命令和cp命令类似，都可以将文件/目录拷贝到指定的地点。但是，***install允许你控制目标文件的属性***。install通常用于程序的makefile，使用它来***将程序拷贝到目标（安装）目录。***

install [xx] soureFiles distDir 复制源文件(1-n)到目的目录

install [xx] soureFile distFile 复制源文件(1)到目的文件

insatll [xx] -t distDir sourceFile

install [xx] -d Dir 创建指定目录

选项-g表示设置所属组

选项-m表示设置模式(chmod)

选项-o表示设置所有者

**nl命令:(类似cat –n)** 读取file，并标定行号。

nl filename

**fmt命令**:读取文件的内容，根据选项的设置对*文件格式进行简单的优化处理*，并将结果送到标准输出设备。

fmt [xx] filename

选项-w<每列字符数>：设置每列的最大字符数。

选项-s：只拆开字数超出每列字符数的列，但不合并字数不足每列字符数的列；

**bzip2命令:** 解压缩指定的.bz2文件，并显示解压缩后的文件内容。保留原压缩文件，并且不生成解压缩后的文件。

bzip2 (参数) file.bz2

参数-z压缩

参数-d强制解压缩bz文件

参数-k保留源文件

参数-v压缩过程

参数-t测试压缩

**zipsplit命令:** 用于将较大的“zip”压缩包分割成各个较小的“zip”压缩包

zipsplit [xx] filename

选项-n指定分割后每个zip文件的大小

选项-b指定分割后的文件位置

**unzip命令:** 用于解压缩由zip命令压缩的“.zip”压缩包

unzip [xx] file.zip

选项-n：解压缩时不要覆盖原有的文件；  
 选项-d<目录>：指定文件解压缩后所要存储的目录；  
 选项-v：执行时显示详细的信息；

选项-o：不必先询问用户，unzip执行后覆盖原有的文件；

选项-P<密码>：使用zip的密码选项；

**zip命令:**可以用来解压缩文件，或者对文件进行打包操作。zip是个使用广泛的压缩程序，文件经它压缩后会另外产生具有“.zip”扩展名的压缩文件。

zip [xx] file.zip file(s)

选项-q：不显示指令执行过程；

选项-r：递归处理，将指定目录下的所有文件和子目录一并处理；

选项-b<工作目录>：指定暂时存放文件的目录；

选项-d：从压缩文件内删除指定的文件；

**zipinfo命令：**用来列出压缩文件信息。执行zipinfo指令可得知zip压缩文件的详细信息

zipinfo [xx] file.zip

**tar命令:**可以为linux的文件和目录创建档案。利用tar，可以为某一特定文件创建档案（***备份文件***），也可以在档案中***改变文件***，或者向档案中***加入新的文件***。tar最初被用来在磁带上创建档案，现在，用户可以在任何设备上创建档案。利用tar命令，可以把一大堆的文件和目录全部打包成一个文件，这对于备份文件或将几个文件组合成为一个文件以便于网络传输是非常有用的。

tar [xx] file.tar files(dirs)

选项-r：添加文件到已经压缩的文件；

选项-p：用原来的文件权限还原文件

选项-C <目录>：***这个选项用在解压缩，若要在特定目录解压缩，可以使用这个选项。***

选项-t或--list：列出备份文件的内容；

选项-g <snapshot>: 文件增量备份,snapshot为备份快照文件

选项-k : 保留原有文件不被覆盖

选项-m：保留文件不被覆盖

**顺序不能颠倒:(文件全备份和增量备份)**

tar –g /tmp/snapshot -zvcf data.tar.gz data/ 全备份

tar –g /tmp/snapshot -zvxf add.tar.gz data/ 增量备份

选项-c或--create：建立新的备份文件；

选项-x从备份文件中还原文件；

选项-v显示指令执行过程；

选项-f：指定备份文件

选项-z通过gzip指令处理备份文件；

选项-j：支持bzip2解压文件；

压缩: -zvcf ----> tar.gz -jvcf ---->tar.bz

-vcf------->tar

解压: -zvxf ----->解压tar.gz -jvxf---->解压tar.bz

-vxf------->解压tar

查看: -zvtf------>查看tar.gz -jvtf----->查看tar.bz

-vtf-------->查看tar

添加： -vrf-------->tar(其他的添加不可以)

**comm命令:**可以用于***两个文件***之间的比较，它有一些选项可以用来调整输出，以便执行交集、求差、以及差集操作。

交集：打印出两个文件所共有的行。

求差：打印出指定文件所包含的且不相同的行。

差集：打印出包含在一个文件中，但不包含在其他指定文件中的行。

comm [xx] file1 file2

选项-1：不显示在第一个文件出现的内容；

选项 -2：不显示在第二个文件中出现的内容

选项 -3：不显示同时在两个文件中都出现的内容。

交集：-1 -2

求差：-3

差集：-2 -3

**cmp命令:** 比较***任意两个类型的文件***，且把结果输出到标准输出，默认文件相同不输出，不同的文件输出差异

cmp (必要参数) file1 file2

必要参数

参数-c 显示不同的信息  
参数-l 列出所有的不同信息

**diff命令：比较两个目录**

diff [xx] src\_dir des\_dir

选项 –B 忽略忽略插入删除空行引起的变化.

选项-q仅报告文件是否相异,不报告详细的差异.   
选项-r当比较目录时，递归比较任何找到的子目录

**ftp命令:**用来设置文件系统相关功能。ftp服务器在网上较为常见，Linux ftp命令的功能是用命令的方式来***控制在本地机和远程机之间传送文件***，这里详细介绍Linux ftp命令的一些经常使用的命令，相信掌握了这些使用Linux进行ftp操作将会非常容易。 语法

ftp [xx] ip地址(主机名)

选项-v显示指令执行过程

**scp命令**:用于在Linux下进行***远程拷贝文件的命令***，和它类似的命令有cp，不过cp只是在本机进行拷贝不能跨服务器，而且scp传输是加密的。另外，scp还非常不占资源，不会提高多少系统负荷

scp [xx] source UserName@Host:dist (两者可以交换)

选项-r：以递归方式复制。

选项-C：使用压缩；

选项-o：指定使用的ssh选项；

选项-P：指定远程主机的端口号

**rcp命令:**使在两台Linux主机之间的文件复制操作更简单。通过适当的配置，在两台Linux主机之间复制文件而无需输入密码，就像本地文件复制一样简单。

开启rcp命令：(root用户)

1、在双方root用户根目录下建立rhosts文件，并将双方的hostname加进去。***在此之前应在双方的/etc/hosts文件中加入对方的ip和hostname***。

2、把rsh服务启动起来，redhat默认是不启动的。 方法：用执行ntsysv命令，在rsh选项前用空格键选中，确定退出。然后执行service xinetd restart即可。

3、到/etc/pam.d/目录下，把rsh文件中的auth required /lib/security/pam\_securetty.so一行用“#”注释掉即可。（只有注释掉这一行，才能用root用户登录）

rcp [xx] source Host:dist (两者可以交换)

选项-p：保留源文件或目录的属性，包括拥有者、所属群组、权限与时间； 选项-r：递归处理，将指定目录下的文件与子目录一并处理；

chmod命令:用来变更文件或目录的***权限***

权限范围的表示法如下：

u User，即文件或目录的拥有者；

g Group，即文件或目录的所属群组；

o Other，除了文件或目录拥有者或所属群组之外，其他用户皆属于这个范围；

a All，即全部的用户，包含拥有者，所属群组以及其他用户；

r 读取权限，数字代号为“4”;

w 写入权限，数字代号为“2”；

x 执行或切换权限，数字代号为“1”；

- 不具任何权限，数字代号为“0”；

s 特殊功能说明：变更文件或目录的权限。

chmod [xx] file(dir)

选项-R：递归处理，将指令*目录下的所有文件及子目录一并处理*；

选项-v或——verbose：显示指令执行过程；

**chown命令:**改变某个文件或目录的***所有者和所属的组***，该命令可以向某个用户授权，使该用户变成指定文件的所有者或者改变文件所属的组。用户可以是用户或者是用户D，用户组可以是组名或组id。文件名可以使由空格分开的文件列表，在文件名中可以包含通配符.

chown [xx] 用户:组 file(dir)

选项-h：只对符号连接的文件作修改，而不更改其他任何相关文件；

选项-R：递归处理，将指定***目录***下的所有文件及子目录一并处理；

选项-v：显示指令执行过程；

**chgrp命令:**用来改变文件或目录所属的***用户组***。该命令用来改变指定文件所属的用户组。

chgrp [xx] 组 file(dir)

选项-h：只对符号连接的文件作修改，而不更改其他任何相关文件；

选项-R：递归处理，将指定***目录***下的所有文件及子目录一并处理；

选项-v：显示指令执行过程；

**stat命令:**用于***显示文件的状态信息***。stat命令的输出信息比ls命令的输出信息要更详细。

stat [xx] file

选项-L：支持符号连接；

选项-t：以简洁方式输出信息；

**cp命令**:用来将一个或多个源文件或者目录复制到指定的目的文件或目录

cp [xx] source dist

选项-r：递归处理，将指定**目录**下的所有文件与子目录一并处理；

选项-d：当复制符号连接时，把目标文件或目录也建立为符号连接，并指向与源文件或目录连接的原始文件或目录；

选项-s：对源文件建立符号连接，而非复制文件；

选项-l：对源文件建立硬连接，而非复制文件

**ln命令**：用来为文件创件连接，连接类型分为硬连接和符号连接两种，默认的连接类型是硬连接。如果要创建符号连接必须使用"-s"选项。

ln [xx] source distFile

source：指定连接的源文件。*如果使用-s选项创建符号连接，则“源文件”可以是文件或者目录。*创建硬连接时，则“源文件”参数只能是文件；

选项-d：建立目录的硬连接；

选项-f：强行建立文件或目录的连接，不论文件或目录是否存在；

选项-s：对源文件建立符号连接，而非硬连接；

选项-n：把符号连接的目的目录视为一般文件；

## 2.系统管理

**runlevel命令**:用于打印当前Linux系统的运行等级。

0 停机

1 单用户模式

2 多用户，没有 NFS

3 完全多用户模式

4 没有用到

5 图形界面

6 重新启动

**telint命令**:用于切换当前正在运行的Linux系统的运行等级。

telint [xx] level

选项-t：指定等待的秒数

**ps命令**:用于报告当前系统的进程状态。可以搭配kill指令随时中断、删除不必要的程序。

ps //当前用户的进程

ps -ef //系统所有的进程及其状态

**pkill命令:**可以***按照进程名杀死进程***。pkill和killall应用方法差不多，也是直接杀死运行中的程序；如果您想杀掉单个进程，请用kill来杀掉.

pkill [xx] 进程名称

选项-g：指定进程组；

选项-t：指定开启进程的终端

**kill命令**:用来删除执行中的程序或工作。kill可将指定的信息送至程序

kill [xx] PID

选项-p：指定kill 命令只打印相关进程的进程号，而不发送任何信号

kill -l 用于查询所有的信号名称

kill -9 PID 彻底杀死进程

kill –KILL PID 强制杀死进程

kill -u user 杀死user用户的所有进程

## 3.网络管理

**axel:** 是Linux下一个不错的HTTP/ftp高速下载工具。支持***多线程下载、断点续传***，且可以从***多个地址或者从一个地址的多个连接来下载同一个文件***。适合网速不给力时多线程下载提高下载速度。

安装：(64位CentOS)

wget –c <http://pkgs.repoforge.org/axel/axel-2.4-1.el5.r-f.x86_64.rpm>

rpm -ivh axel-2.4-1.el5.rf.x86\_64.rpm

安装：(Debian/Ubuntu)

apt-get install axel

axel [xx] url1 [urlx]

选项 –n x 连接数x

选项 –o f 下载为本地文件f

**ssh命令：**

ssh host 当前用户登陆host

ssh host -l username 以username的身份登陆host

ssh user@host –p xx 指定端口登陆

ssh -D xxx user@host 通过远程代理登陆

ssh host command 远程执行命令

ssh -n –q -l username host 远程登陆

**ping命令:网络或者主机直接的连通性测试,默认字节大小为64bit,**

**rtt是发送到回来的时间**

ping [xx] (IP|DOMAIN)

选项-c <num> 指发送num个ping包(默认一直发送)

选项-s <packsize> 指定ping包大小

选项-W <time> 等待的最大回应时间,如果不回复则终止

选项-w <time> ping的时间,time秒后结束ping

**route命令:管理路由表,GateWay是网关地址,Destination是目标地址**

route -n 查看路由表

route add (-net|-host)DESTINATION [netmask Num] gw GATEWAY

添加一个路由器网关.-net是网络路由,-host是主机路由,DESSTINATION是目标地址.netmask是掩码位数(主机可以忽略),gw是经过的路由地址,这个值需要和本机在同一个网段.

route del (-net|-host) DESTINATION [netmask NUM]

删除路由.

**ssh-keygen命令:**用于为“ssh”生成、管理和转换认证密钥，它支持RSA和DSA两种认证密钥

ssh-keygen [xx]

选项-t：指定要创建的密钥类型。(RSA,DSA)

选项-b：指定密钥长度；

选项-e：读取openssh的私钥或者公钥文件

**ssh-copy-id命令:**可以把***本地主机的公钥***复制到远程主机的authorized\_keys文件上，ssh-copy-id命令也会给远程主机的用户主目录（home）和~/.ssh, 和~/.ssh/authorized\_keys设置合适的权限。

ssh-copy-id -i rsa\_pub\_file user@从机IP

**ssh-add命令**:是把***专用密钥添加到ssh-agent的高速缓存中***。该命令位置在/usr/bin/ssh-add

ssh-add [xx]

选项 file :添加file中的公钥到高速缓存中

选项-d file：从ssh-agent中的删除file中的密钥

选项-L：显示ssh-agent中的公钥

选项-l：显示ssh-agent中的密钥

**ssh-keyscan命令**:是一个收集大量主机公钥的使用工具

ssh-keysacn 主机列表(要收集公钥的主机)

ssh-keyscan –f file 从file(主机地址列表文件)中收集主机公钥

**wget命令**用来从指定的URL下载文件。

wget [xx] url

选项-b：进行后台的方式运行wget

选项-A<后缀名>：指定要下载文件的后缀名，多个后缀名之间使用逗号进行分隔；

选项-r：递归下载方式

**sftp命令**是一款交互式的文件传输程序

sftp [xx] host(指定sftp服务器ip地址或者主机名)

选项-B：指定传输文件时缓冲区的大小

选项-o:指定ssh选项

选项-C:使用压缩

**mail命令**:是命令行的电子邮件发送和接收工具。

mail [xx] address

选项-s<邮件主题>：指定邮件的主题；

选项-u<用户帐号>：读取指定用户的邮件；

选项-I：使用互动模式；

选项-f <发送人邮件地址>

选项-c<抄送地址>

邮件发送：

管道方式:

echo “xxxxxxx” | mail –s “subject” [xx@xxx.com](mailto:xx@xxx.com)

文本方式:

mail -s “subject” [xx@xxx.com](mailto:xx@xxx.com) < file.txt

普通方式:

mail -s “subject” [xx@xxx.com](mailto:xx@xxx.com)

回车,然后输入文件内容，并按CTrl+D结束，然后回车

**netstat命令**用来打印Linux中网络系统的状态信息，可让你得知整个Linux系统的网络情况

netstat [xx]

选项-a 显示所有连线中的Socket

选项-c或--continuous：持续列出网络状态；

选项-l或--listening：显示监控中的服务器的Socket

选项-n或—numeric:直接使用ip地址,而不通过域名服务器；

选项-t或--tcp：显示TCP传输协议的连线状况；

选项-u或--udp：显示UDP传输协议的连线状况；

选项-s：显示网络工作信息统计表(与-u –t结合使用)

选项-r或--route：显示Routing Table；(路由表)

选项-i或--interfaces：显示网络界面信息表单；

**chkconfig命令**检查、设置系统的各种服务

chkconfig xxx on/off 开启或关闭服务

chkconfig --list 列出所有的服务

chkcongit --add/--del xx 添加或删除服务

chkconfig --level xx n on/off设置服务在级别n开启/关闭

**yum命令**是在Fedora和RedHat以及SUSE中基于rpm的软件包管理器，它可以使系统管理人员交互和自动化地更细与管理RPM软件包，能够从指定的服务器自动下载RPM包并且安装，可以自动处理依赖性关系，并且一次安装所有依赖的软体包，无须繁琐地一次次下载、安装。

yum [xx] (参数)

选项-y：对所有的提问都回答“yes”；

参数install：安装rpm软件包；

参数update：更新rpm软件包；

参数remove：删除指定的rpm软件包；

参数list：显示软件包的信息；

参数search：检查软件包的信息；

参数info：显示指定的rpm软件包的描述信息和概要信息；

参数clean：清理yum过期的缓存；

参数shell：进入yum的shell提示符；

参数resolvedep：显示rpm软件包的依赖关系；

参数localinstall：安装本地的rpm软件包；

**rpm命令**是RPM软件包的管理工具。

rpm -ivh 软件包 #安装软件包

rpm -i URL #在线安装

rpm -e 软件名 #卸载软件

rpm -qa #列出所有安装过的包

rpm -ql 软件包 #查看rpm软件包安装的位置

rpm -qf `which 命令` #返回软件包的全名

**who命令**是显示目前登录系统的用户信息

who [xx]

选项-q只显示登入系统的帐号名称和总人数；

选项-H：显示各栏位的标题信息列；

选项-w：显示用户的信息状态栏；

**sum命令**用于计算并显示指定文件的校验和与文件所占用的磁盘块数

sum [xx] file

选项-r：使用BSD的校验和算法，块大小为1k；

选项-s：使用system V的校验和算法，块大小为512字节

## 4.系统管理

**sudo命令**:用来以其他身份来执行命令，预设的身份为root。**在/etc/sudoers中设置了可执行sudo指令的用户**。若其未经授权的用户企图使用sudo，则会发出警告的邮件给管理员。用户使用sudo时，必须先输入密码，之后有5分钟的有效期限，超过期限则必须重新输入密码。

sudo -i [command] 以root用户身份运行command

sudo -i 登陆root用户

sudo -u <user> commnad 以user用户身份运行command

sudoedit –u <user> file 以user用户身份编辑file

sudo -v 更新用户的时间戳而不执行命令

关于/etc/sudoers文件的配置：

foobar ALL=(ALL) ALL

第一个ALL是指网络中的主机，它指明foobar可以在此主机上执行后面的命令。

第二个括号里的ALL是指目标用户，也就是以谁的身份去执行命令。

最后一个ALL当然就是指命令名了。

**shudown命令:关机**

**shutdown -h now 系统立即关机**

**shutdown -h TIME 在TIME时刻系统自动关机**

**shutdown -r now 立即重启**

**shutdown -r +n 在n分钟之后系统重启**

**shutdown -c 取消关机或者重启命令**

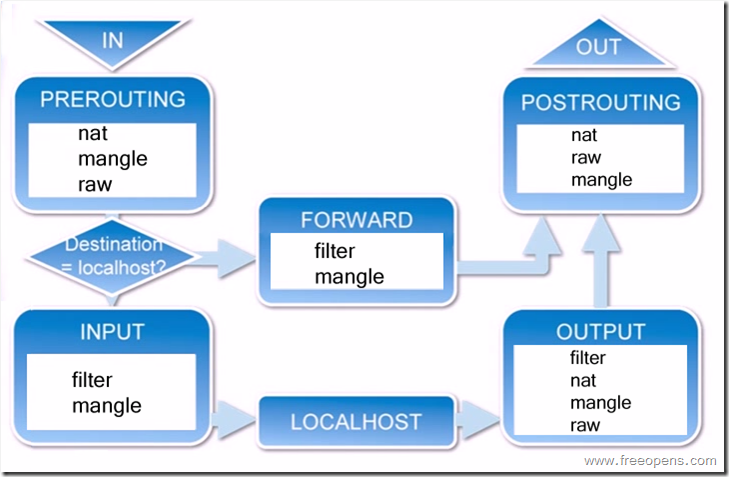
## 5.防火墙介绍

**原理：**

① 当一个数据包进入网卡时，它首先进入PREROUTING链，内核根据数据包目的IP判断是否需要转送出去。

② 如果数据包就是进入本机的，它就会沿着图向下移动，到达INPUT链。数据包到了INPUT链后，任何进程都会收到它。本机上运行的程序可以发送数据包，这些数据包会经过OUTPUT链，然后到达POSTROUTING链输出。

③ 如果数据包是要转发出去的，且内核允许转发，数据包就会如图所示向右移动，经过FORWARD链，然后到达POSTROUTING链输出。



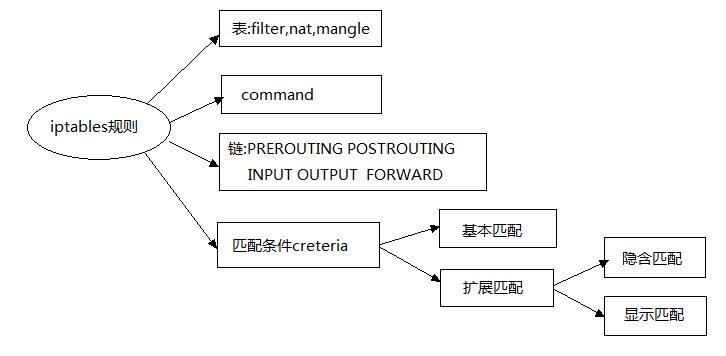
**iptables [-t table] command chains [creteria] -j action**

-t table就是表名，filter/nat/mangle三个表中的一个，默认是filter表

command告诉程序如何做，例如：插入一个规则，还是删除等

chains 链有五个，PREROUTING POSTROUTING INPUT OUTPUT FORWARD

action 处理动作，有ACCEPT DENY DROP REJECT SNAT DNAT



-t table

Filter:专门过滤包的内建三个链,INPUT OUTPUT FORWARD

INPUT专门针对那些目的是本地的包；OUTPUT是用来过滤所有本地生产的包；FORWARD过滤所有不是本地生产的且目的地不是本地的包

nat:主要用于网络地址转换。PREROUTING链的作用是在包刚刚到达防火墙时改变他的目的地址。OUTPUT改变本地生产的包的目的地址;POSTROUTING在包就要离开防火墙之前改变其源地址

mangle:主要用来操作数据包的。可以改变不同的包或包头的内容。

command

command指定iptables对我们提价的规则要做什么样的操作。这些操作可能是在某个表里增加或删除一些东西，或其他的动作。以下是iptables可用的command(如果不说明，默认表是filter)

-A(--append) iptables –A INPUT …

在所选择的链末添加规则

-D(--delete) iptables –D INPUT 2

在所选择的链中删除规则，指定所选中链的序号

-I(--insert) iptables –I INPUT 2…

在所选择的链中插入规则

-R(--replace) iptables –R INPUT 1…

在所选中的链中指定的行上替换规则

-N(--new-chain) iptables –N allow

新建用户自定义链

-F(--flush) iptables –F INPUT

清空所选中的链，若没有指定链，则清空所选表的所有链

-X(--delete-chain) iptables –X allow

删除指定的用户自定义链。这个链必须没有被引用，若引用，则先删除

-Z(--zero) iptables –Z INPUT

把指定链中所有计数器归零

-E(--rename-chain) iptables –E allow disallow

对自定义的链重命名

-P(--policy) iptables –P INPUT DROP

设置默认策略

-L(--list) iptables –L INPUT

显示所选中链的所有规则，会经常和-n –v结合使用

和命令结合常用的选项:(--list)

-v(--verbose) 详细的 显示详细信息

-n(--numeric) 数值 使输出的ip地址和端口号以数字

值的形式显示。

-x(--exact) 显示计数器准确值

--line-numbers 显示每条规则在相应链中的序号

chains

简单说一下五个链的作用：

PREROUTING 是在包进入防火墙之后、路由决策之前做处理

POSTROUTING 是在路由决策之后，做处理

INPUT 在包被路由到本地之后，但在出去用户控件之前做处理

OUTPUT在去顶包的目的之前做处理

FORWARD在最初的路由决策之后，做转发处理

匹配条件

**基本匹配**(源地址目标地址的匹配)



**扩展匹配**

**隐含扩展：**对协议的扩展

TCP匹配:只能匹配TCP包的细节，必须有-p tcp作为前提

--dport xx 基于TCP包的目的端口来匹配包

--dport xx-yy 指定多个连续的端口号

--sport xx 基于TCP包的源端口来匹配包

UDP匹配：必须有-p udp作为前提

--sprot xx

--dport xx

ICMP匹配：必须有-p icmp作为前提(ping配置)

--icmp-type 0(8)

echo-request(请求回显)，一般用8 来表示

echo-reply （响应的数据包）一般用0来表示

**显示扩展:**扩展各模块

-m multiport：表示启用多端口扩展

**--source-ports   
        --destination-ports   
        --ports**

state:状态扩展，结合ip\_conntrack追踪会话的状态，ip状

态有四种

--state NEW：新连接请求

--state ESTABLISHED：已建立的连接

--state INVALID：非法连接

--state RELATED：相关联的

iprange指定IP地址段（指定地址池），也可以取反“！

--src-range

--dst-range

-j ACTION

常用的ACTION：

DROP:**悄悄丢弃，一般我们多用DROP来隐藏我的身份，以及隐藏我们的链表**

REJECT：**明示拒绝**

ACCEPT：**接受**

DNAT: **目标地址转换(**一般在PREROUTING链上操作)

SNAT: **源地址转换(**一般在POSTROUTING链上操作)

MASQUERADE：**源地址伪装**

REDIRECT：**重定向：主要用于实现端口重定向**

MARK：**打防火墙标记的**

RETURN：**返回在自定义链执行完毕后使用返回，来返回原规则链**

**给SSH加放行的语句:(机器在身边)**

添加input记录:iptables -A INPUT -p tcp --dport 22 -j ACCEPT

添加output记录iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

再执行一下/etc/init.d/iptables save，这样这两条语句就保存到刚才那个/etc/sysconfig/iptables文件中了。

**给SSH加放行的语句:(机器不在身边)**

首先要做的是给咱的SSH进行ACCEPT配置，以免直接无法连接的情况发生:

1.如果SSH端口是22

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

**注意**:要/etc/rc.d/init.d/iptables save，以下每一步都最好执行一遍此语句，以下不再累述。

2.vim /etc/sysconfig/iptables确定是否已经加入配置，可以的话执行service iptables restart重启后生效

3.下面是很危险的操作，如果你第一步没做就会直接可能导致你连不上SSH，此步骤前切记执行第一步！！！

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

这个步骤是把所有不符合自己配置的规则ACCEPT的连接全部DROP掉，执行完以后如果咱SSH还没掉，那么谢天谢地，安全了，重启下iptables后继续下面的配置！

**例子：**

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#ping使用的端口

-A INPUT -p icmp -j ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT

-A INPUT -s 192.168.2.200/32 -d 192.168.2.200/32 -j ACCEPT

#允许服务器自己的SSH（对外部请求来说服务器是目标所以使用--dport）

-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT

#80端口不用说了吧，服务器网站访问端口

-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 3306 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 11211 -j ACCEPT

-A INPUT -p tcp -m tcp --dport 11212 -j ACCEPT

-A FORWARD -j REJECT --reject-with icmp-host-prohibited

#53端口是DNS相关，TCP和UDP都要配置

-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT

-A INPUT -p udp -m udp --dport 53 -j ACCEPT

#ping使用的端口

-A OUTPUT -p icmp -j ACCEPT

-A OUTPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT

-A OUTPUT -s 192.168.2.200/32 -d 192.168.2.200/32 -j ACCEPT

#允许服务器SSH到其他机器（使用外部端口就使用--dport）

-A OUTPUT -p tcp -m tcp --dport 22 -j ACCEPT

#允许服务器自己的SSH（自已为源输出就使用--sport）

-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT

#访问外部网站80端口（使用外部端口就使用--dport）

-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

#如果服务器需要访问外部网站，那么OUTPUT也需要配置53端口（使用外部端口就使用--dport）

-A OUTPUT -p tcp -m tcp --dport 53 -j ACCEPT

-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT

#如果有访问外部邮箱，那么打开邮箱相关端口（使用外部端口就使用--dport）

-A OUTPUT -p tcp -m tcp --dport 465 -j ACCEPT

-A OUTPUT -p tcp -m tcp --dport 25 -j ACCEPT

-A OUTPUT -p tcp -m tcp --dport 110 -j ACCEPT

#服务器网站访问端口（自已为源输出就使用--sport）

-A OUTPUT -p tcp -m tcp --sport 80 -j ACCEPT

-A OUTPUT -p tcp -m tcp --sport 3306 -j ACCEPT

-A OUTPUT -p tcp -m tcp --sport 11211 -j ACCEPT

-A OUTPUT -p tcp -m tcp --sport 11212 -j ACCEPT

COMMIT

# Completed on Fri Mar 2 19:59:43 2012

**彻底禁止某IP访问:**

#屏蔽单个IP的命令是

iptables -I INPUT -s 123.45.6.7 -j DROP

#封整个段即从123.0.0.1到123.255.255.254的命令

iptables -I INPUT -s 123.0.0.0/8 -j DROP

#封IP段即从123.45.0.1到123.45.255.254的命令

iptables -I INPUT -s 124.45.0.0/16 -j DROP

#封IP段即从123.45.6.1到123.45.6.254的命令是

iptables -I INPUT -s 123.45.6.0/24 -j DROP

指令I是insert指令 但是该指令会insert在正确位置并不像A指令看你自己的排序位置，因此用屏蔽因为必须在一开始就要加载屏蔽IP，所以必须使用I命令加载，然后注意执行/etc/rc.d/init.d/iptables save进行保存后重启服务即可

**SNAT策略概述：**

网络基础知识：**IP地址、子网掩码、网关、DNS的关系**

**IP地址**，标示你电脑的身份。**子网掩码**，可以标示子网划分的情况，所属子网。**默认网关**，数据包默认选择的出口，一般是你的路由器地址！**DNS服务器**，把网站的域名转换成计算机能看懂的IP地址。

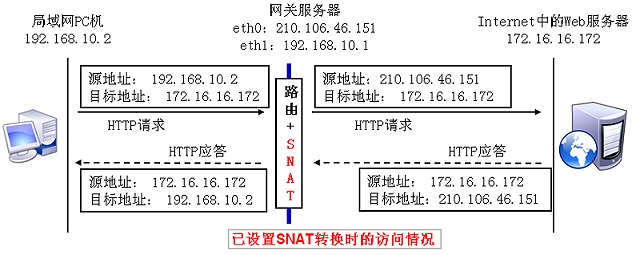
简单来说，子网掩码 就是判断两个IP地址，是不是在同一个网段(或称子网)，**在同一网段的两个地址**，可以直接通信。不管是通过IP地址也好，还是通过“计算机名”，都是可以的。**如果两个IP地址，不在同一网段**，这时候，要想通过IP地址访问另一网段的计算机(也是IP地址)，就需要网关地址。网关地址就是出口的地址，而且，网关地址，是你最近的一个出口的地址。***网关地址总是与你的计算机的IP地址是同一网段的。***如果两台计算机，不在同一网段，如果想使用计算机名(就是类似于compute1、cp2之类的名称，称为NetBIOS名称)，这时候，必须要使用WINS服务器来解析(或者手动编辑本机的hosts文件)

***SNAT策略的典型应用环境***(客户端的网关服务器)

局域网客户机共享单个公网IP地址接入Internet中的web服务器

**SNAT策略的原理：**

**源地址转换**（Source Network Address Translation）是linux防火墙的一种地址转换操作，也是iptables命令中的一种数据包控制类型，并根据指定条件修改数据包的源IP地址。



配置：

1. 启用网关的路由转发

永久打开

vim /etc/sysctl.conf

将net.ipv4.ip\_forward 设置为1

临时开启

vim /proc/sys/net/ipv4/ip\_forward

将其内容改为1

2. 设置SNAT策略

iptables -t nat -A POSTROUTING –s IP(局域IP带掩码)

–o 外网网卡 –j SNAT --to-source IP地址(外网IP)

iptables -A INPUT –p tcp –dport xx –j ACCEPT

***共享动态IP地址上网****:* (MASQUERADE—— 地址伪装)

* 适用于外网IP地址非固定的情况
* 对于ADSL拨号连接，接口通常为ppp0、ppp1
* 将SNAT规则改为MASQUERADE即可

设置MASQUERADE策略

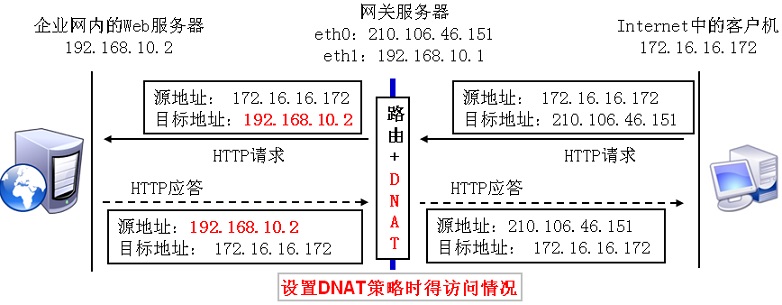
iptables -t nat -A POSTROUTING –s 源IP(局域IP带掩码) –o ppp0 –j MASQUERADE

***DNAT策略的典型应用环境***(服务器)

**web服务器在接入Internet的局域网中**

**DNAT策略的原理**

**目标地址转换**，Destination Network Address Translation，是Linux防火墙的另一种地址转换操作，也是iptables命令中的一种数据包控制类型，其作用是根据指定条件修改数据包的目标IP地址、目标端口。

**SNAT用来修改源IP地址，而DNAT用来修改目标IP地址、目标端口；SNAT只能用在nat表的POSTROUTING链，而DNAT只能用在nat表的PREROUTING链和OUTPUT链（或被其调用的链）中。**

配置：

1. 启用网关的路由转发

永久打开

vim /etc/sysctl.conf

将net.ipv4.ip\_forward 设置为1

临时开启

vim /proc/sys/net/ipv4/ip\_forward

将其内容改为1

2. 局域网内主机共享一个共有IP地址访问Internet(响应过程)

iptables –t nat –A POSTROUTING –s 局域网IP(掩码)

-o 外网网卡 –j SNAT --to-source 外网IP

Internet可以访问公司的网站(请求过程)

iptables –t nat –A　PREROUTING –i 外网网卡 –d 外网IP –p tcp –j DNAT –-to 局域网具体IP

3.设置DNAT策略：

管理员在外网可远程管理公司web服务器(不使用标准端口)

iptables -t nat -A PREROUTING –i 外网网卡 -d 外网IP -p tcp --dport 端口 -j DNAT --to-destination 局域网具体IP:端口