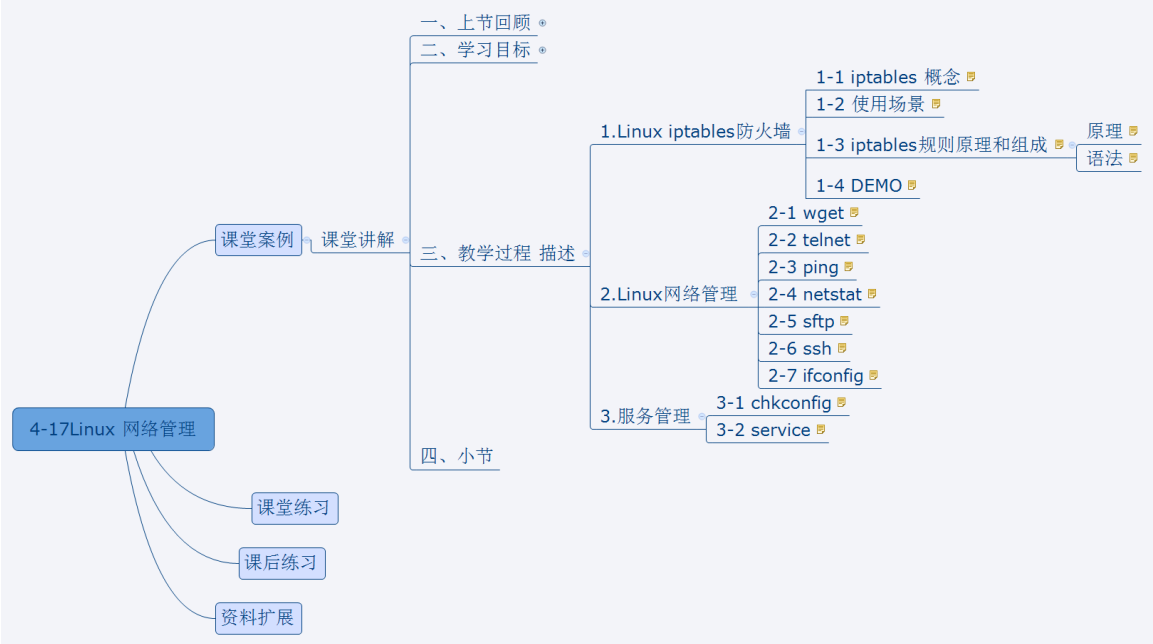
4-17Linux 网络管理



1. 课堂案例

课堂讲解

一、上节回顾

系统管理

压缩解压命令

软件管理命令

权限管理

二、学习目标

防火墙设置

网络配置及管理

服务管理

三、教学过程 描述

1.Linux iptables防火墙

1-1 iptables 概念

什么是iptables?

iptables 是一个linux下的应用层防火墙工具? 可以想像成小区的保安？

谁会使用iptables?

一般是运维人员，我们的软件工程师也会使用iptables 来控制对一些服务器访问限制

1-2 使用场景

使用iptables 控制web 高并发，比如，将并发控制在10个，多余的并发打拒绝响应

1-3 iptables规则原理和组成

介绍 iptables 前介绍两个概念

netfilter

什么是Netfilter?

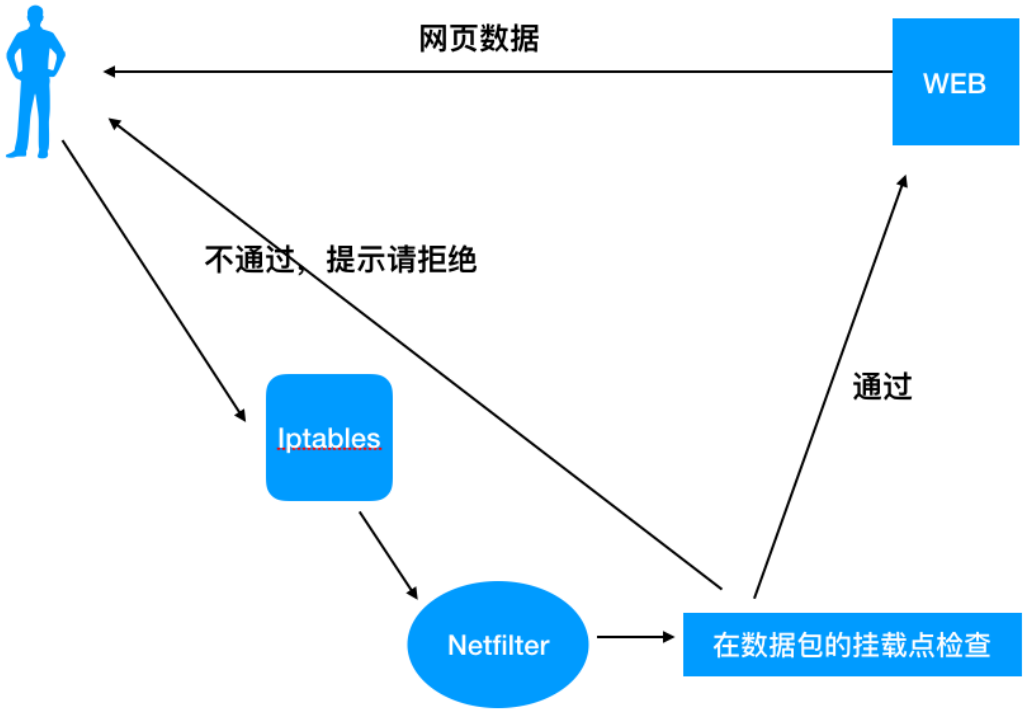
Netfilter 是Linux 操作系统内核中的用于数据包的模块

什么是 Hook point?

数据包在 Netfilter中的挂载点（PRE_ROUTING, INPUT,OUTPUT,FORWARD,POST_ROUTING）

意思就是，那些地方要对数据包进行过虑，就好比高速公路上的收费站

原理



四张表 + 五条链（Hook point）+ 规则

iptable 中四张表：

raw：高级功能，如：网址过滤。

mangle：数据包修改（QOS），用于实现服务质量。

net：地址转换，用于网关路由器。

filter：包过滤，用于防火墙规则。

五条链就是：5个挂载点：

1.PREROUTING (路由前)

2.INPUT (数据包流入口)

3.FORWARD (转发管卡)

4.OUTPUT(数据包出口)

5.POSTROUTING（路由后）

防火墙的策略:

1. 通 策略（默认是关着的）也就是说默认情况下谁都不允许通过，必须定义谁能从这过

2. 堵 策略　意思是大门是洞开的，但是你必须有身份认证，否则不能进

因此我们要定义让谁能进来或是谁能出去

语法

iptables【选项】参数

选项:

-t <表>:指定要操纵的表;

-A:向规则链中添加条目;

-D:从规则链中删除条目;

-i:向规则链中插入条目;

-R:替换规则链中的条目;

-L:显示规则链中已有的条目;

-F:清楚规则链中已有的条目;

-Z:清空规则链中的数据包计算器和字节计数器;

-N:创建新的用户自定义规则链;

-P:定义规则链中的默认目标;

-h:显示帮助信息;

-p:指定要匹配的数据包协议类型;

-s:指定要匹配的数据包源ip地址;

-j<目标>:指定要跳转的目标;

-i<网络接口>:指定数据包进入本机的网络接口;

-o<网络接口>:指定数据包要离开本机所使用的网络接口。

iptables命令选项输入顺序:

iptables -t 表名 <-A/I/D/R> 规则链名 [规则号] <-i/o 网卡名> -p 协议名 <-s 源IP/源子网> --sport 源端口 <-d 目标IP/目标子网> --dport 目标端口 -j 动作

表名包括:

raw:高级功能，如:网址过滤。

mangle:数据包修改(QOS),用于实现服务质量。

net:地址转换,用于网关路由器。

filter:包过滤,用于防火墙规则。

规则链名包括:

INPUT链:处理输入数据包。

OUTPUT链:处理输出数据包。

PORWARD链:处理转发数据包。

PREROUTING链:用于目标地址转换(DNAT)。

POSTOUTING链:用于源地址转换(SNAT)。

动作包括:

accept:接收数据包。

DROP:丢弃数据包。

REDIRECT:重定向、映射、透明代理。

SNAT:源地址转换。

DNAT:目标地址转换。

MASQUERADE:IP伪装(NAT),用于ADSL。

LOG:日志记录。

1-4 DEMO

开启: chkconfig iptables on

关闭: chkconfig iptables off

清除已有iptables规则

iptables -F

iptables -X

iptables -Z

开放指定的端口

iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -j ACCEPT #允许本地回环接口(即运行本机访问本机)

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT #允许已建立的或相关连的通行

iptables -A OUTPUT -j ACCEPT #允许所有本机向外的访问

iptables -A INPUT -p tcp --dport 22 -j ACCEPT #允许访问22端口

iptables -A INPUT -p tcp --dport 80 -j ACCEPT #允许访问80端口

iptables -A INPUT -p tcp --dport 21 -j ACCEPT #允许ftp服务的21端口

iptables -A INPUT -p tcp --dport 20 -j ACCEPT #允许FTP服务的20端口

iptables -A INPUT -j reject #禁止其他未允许的规则访问

iptables -A FORWARD -j REJECT #禁止其他未允许的规则访问

屏蔽IP

iptables -I INPUT -s 123.45.6.7 -j DROP #屏蔽单个IP的命令

iptables -I INPUT -s 123.0.0.0/8 -j DROP #封整个段即从123.0.0.1到123.255.255.254的命令

iptables -I INPUT -s 124.45.0.0/16 -j DROP #封IP段即从123.45.0.1到123.45.255.254的命令

iptables -I INPUT -s 123.45.6.0/24 -j DROP #封IP段即从123.45.6.1到123.45.6.254的命令是

查看已添加的iptables规则

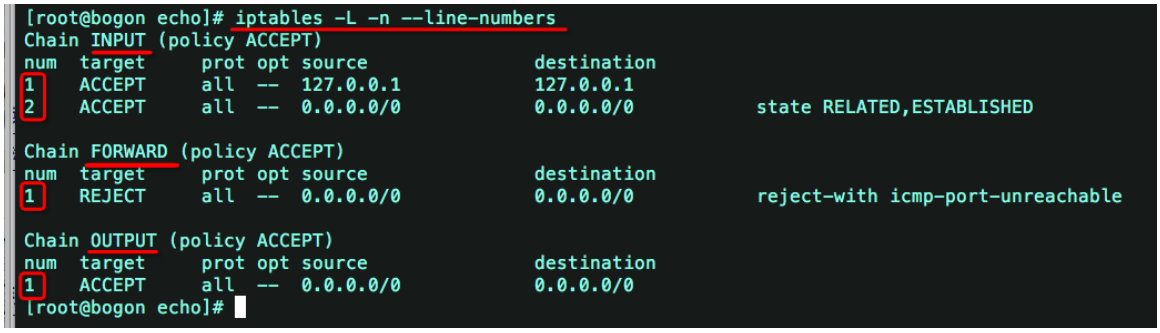
iptables -L -n -v

```
[root@bogon echo]# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       127.0.0.1            127.0.0.1
   65  5364 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   18  3112 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

删除已添加的iptables规则

将所有iptables以序号标记显示，执行：

iptables -L -n --line-numbers



比如要删除INPUT里序号为2的规则，执行：iptables -D INPUT 2

2.Linux网络管理

2-1 wget

wget命令用来从指定的URL下载文件

语法

wget [选项] 参数

选项

-a<日志文件>：在指定的日志文件中记录资料的执行过程；

-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；

-b：进行后台的方式运行wget；

-B<连接地址>：设置参考的连接地址的基地地址；

-c：继续执行上次终端的任务；

-C<标志>：设置服务器数据块功能标志on为激活，off为关闭，默认值为on；

-d：调试模式运行指令；

-D<域名列表>：设置顺着的域名列表，域名之间用“，”分隔；

-e<指令>：作为文件“.wgetrc”中的一部分执行指定的指令；

-h：显示指令帮助信息；

-i<文件>：从指定文件获取要下载的URL地址；

-l<目录列表>：设置顺着的目录列表，多个目录用“，”分隔；

-L：仅顺着关联的连接；

-r:递归下载方式;

-nc:文件存在时,下载文件不覆盖原有文件;

-nv:下载时只显示更新和出错信息,不显示指令的详细执行过程;

-q:不显示指令执行过程;

-nh:不查询主机名称;

-v:显示详细执行过程;

-V:显示版本信息;

--passive-ftp:使用被动模式PASV连接FTP服务器

--follow-ftp:从HTML文件中下载FTP连接文件。

参数 URL:

下载指定的URL地址。

例:

使用wget下载单个文件

wget http://www.linuxde.net/testfile.zip

下载并以不同的文件名保存

wget -O wordpress.zip http://www.linuxde.net/download.aspx?id=1080

wget限速下载

wget --limit-rate=300k http://www.linuxde.net/testfile.zip

使用wget断点续传

wget -c http://www.linuxde.net/testfile.zip

使用wget后台下载

wget -b http://www.linuxde.net/testfile.zip

对于下载非常大的文件的时候,我们可以使用参数-b进行后台下载,

你可以使用以下命令来察看下载进度:

tail -f wget-log

2-2 telnet

telnet命令用于登录远程主机，对远程主机进行管理。

telnet因为采用明文传送报文，安全性不好，

很多Linux服务器都不开放telnet服务，而改用更安全的ssh方式了

语法

telnet [选项] 参数

选项

-8：允许使用8位字符资料，包括输入与输出；

-a：尝试自动登入远端系统；

-b<主机别名>：使用别名指定远端主机名称；

-c：不读取用户专属目录里的.telnetrc文件；

-d：启动排错模式；

-e<脱离字符>：设置脱离字符；

-E：滤除脱离字符；

-f：此参数的效果和指定"-F"参数相同；

-F：使用Kerberos V5认证时，加上此参数可把本地主机的认证数据上传到远端主机；

-k<域名>：使用Kerberos认证时，加上此参数让远端主机采用指定的领域名，而非该主机的域名；

-K：不自动登入远端主机；

-l<用户名称>：指定要登入远端主机的用户名称；

-L：允许输出8位字符资料；

-n<记录文件>：指定文件记录相关信息；

-r：使用类似rlogin指令的用户界面；

-S<服务类型>：设置telnet连线所需的ip TOS信息；

-x：假设主机有支持数据加密的功能，就使用它；

-X<认证形态>：关闭指定的认证形态。

参数

远程主机：指定要登录进行管理的远程主机；

端口：指定TELNET协议使用的端口号。

实例

telnet 192.168.2.10

Trying 192.168.2.10...

Connected to 192.168.2.10 (192.168.2.10).
Escape character is '^]'.
localhost (Linux release 2.6.18-274.18.1.el5 #1 SMP Thu Feb 9 12:45:44 EST 2012) (1)
login: root
Password: Login incorrect

2-3 ping

ping命令用来测试主机之间网络的连通性

语法
ping(选项)(参数)

选项
-d：使用Socket的SO_DEBUG功能；
-c<完成次数>：设置完成要求回应的次数；
-f：极限检测；-i<间隔秒数>：指定收发信息的间隔时间；
-I<网络界面>：使用指定的网络界面送出数据包；
-l<前置载入>：设置在送出要求信息之前，先行发出的数据包；
-n：只输出数值；
-p<范本样式>：设置填满数据包的范本样式；
-q：不显示指令执行过程，开头和结尾的相关信息除外；
-r：忽略普通的Routing Table，直接将数据包送到远端主机上；
-R：记录路由过程；
-s<数据包大小>：设置数据包的大小；
-t<存活数值>：设置存活数值TTL的大小；
-v：详细显示指令的执行过程。

参数
目的主机：指定发送ICMP报文的目的主机

如：
ping -c 10 www.baidu.com

2-4 netstat

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

语法

netstat【选项】

选项

-a或--all：显示所有连线中的Socket；

-A<网络类型>或--<网络类型>：列出该网络类型连线中的相关地址；

-c或--continuous：持续列出网络状态；

-C或--cache：显示路由器配置的快取信息；

-e或--extend：显示网络其他相关信息；

-F或--fib：显示FIB；

-g或--groups：显示多重广播功能群组组员名单；

-h或--help：在线帮助；

-i或--interfaces：显示网络界面信息表单；

-l或--listening：显示监控中的服务器的Socket；

-M或--masquerade：显示伪装的网络连线；

-n或--numeric：直接使用ip地址，而不通过域名服务器；

-N或--netlink或--symbolic：显示网络硬件外围设备的符号连接名称；

-o或--timers：显示计时器；

-p或--programs：显示正在使用Socket的程序识别码和程序名称；

-r或--route：显示Routing Table；

-s或--statistice：显示网络工作信息统计表；

-t或--tcp：显示TCP传输协议的连线状况；

-u或--udp：显示UDP传输协议的连线状况；

-v或--verbose：显示指令执行过程；

-V或--version：显示版本信息；

-w或--raw：显示RAW传输协议的连线状况；

-x或--unix：此参数的效果和指定"-A unix"参数相同；

--ip或--inet：此参数的效果和指定"-A inet"参数相同。

案例：

列出所有端口 (包括监听和未监听的)

netstat -a #列出所有端口

netstat -at #列出所有tcp端口

netstat -au #列出所有udp端口

列出所有处于监听状态的 Sockets

netstat -l #只显示监听端口

netstat -lt #只列出所有监听 tcp 端口

netstat -lu #只列出所有监听 udp 端口

netstat -lx #只列出所有监听 UNIX 端口

显示每个协议的统计信息

netstat -s 显示所有端口的统计信息

netstat -st 显示TCP端口的统计信息

netstat -su 显示UDP端口的统计信息

在netstat输出中显示 PID 和进程名称

netstat -pt

netstat -p可以与其它开关一起使用，就可以添加“PID/进程名称”到netstat输出中，这样debugging的时候可以很方便的发现特定端口运行的程序

在netstat输出中不显示主机，端口和用户名(host, port or user)

当你不想让主机，端口和用户名显示，使用netstat -n。将会使用数字代替那些名称。同样可以加速输出，因为不用进行比对查询。

netstat -an

如果只是不想让这三个名称中的一个被显示，使用以下命令:

netsat -a --numeric-ports

netsat -a --numeric-hosts

netsat -a --numeric-users

持续输出netstat信息

netstat -c #每隔一秒输出网络信息

显示核心路由信息

netstat -r

使用netstat -rn显示数字格式，不查询主机名称。

找出程序运行的端口

并不是所有的进程都能找到，没有权限的会不显示，使用 root 权限查看所有的信息。netstat -ap | grep ssh

找出运行在指定端口的进程:

netstat -an | grep ':80'

显示网络接口列表
netstat -i
显示详细信息，像是ifconfig使用netstat -ie。

2-5 sftp

sftp命令是一款交互式的文件传输程序，命令的运行和使用方式与ftp命令相似，但是，sftp命令对传输的所有信息使用ssh加密，它还支持公钥认证和压缩等功能。

语法 sftp【选项】参数
选项
-B：指定传输文件时缓冲区的大小；
-l：使用ssh协议版本1；
-b：指定批处理文件；
-C：使用压缩；
-o：指定ssh选项；
-F：指定ssh配置文件；
-R：指定一次可以容忍多少请求数；
-v：升高日志等级。

参数
目标主机：指定sftp服务器ip地址或者主机名。
、

例:如远程主机的 IP 是 202.206.64.33或者是域名www.hebust.edu.cn,
用户名是 fyt ,在命令行模式下:
sftp fyt@202.206.64.33
或者
sftp fyt@www.hebust.edu.cn
回车提示输入密码。进入提示符

sftp>

如果登陆远程机器不是为了上传下载文件，而是要修改远程主机上的某些文件。可以

ssh fyt@202.206.64.33（其实sftp就是ssh 的一个程式。）

sftp> get /var/www/fuyatao/index.php /home/fuyatao/
这条语句将从远程主机的 /var/www/fuyatao/目录下将 index.php 下载到本地 /home/fuyatao/目录下。

sftp> put /home/fuyatao/downloads/Linuxgl.pdf /var/www/fuyatao/
这条语句将把本地 /home/fuyatao/downloads/目录下的 linuxgl.pdf文件上传至远程主机/var/www/fuyatao/ 目录下。

你如果不知道远程主机的目录是什么样,
pwd命令可以帮您查询远程主机的当前路径。查询本机当前工作目录 lpwd.

退出sftp,
exit
或
quit、bye 均可

2-6 ssh

ssh命令是openssh套件中的客户端连接工具，可以给予ssh加密协议实现安全的远程登录服务器。

语法 ssh【选项】参数
选项
-1：强制使用ssh协议版本1；
-2：强制使用ssh协议版本2；
-4：强制使用IPv4地址；
-6：强制使用IPv6地址；
-A：开启认证代理连接转发功能；
-a：关闭认证代理连接转发功能；
-b：使用本机指定地址作为对应连接的源ip地址；
-C：请求压缩所有数据；
-F：指定ssh指令的配置文件；
-f：后台执行ssh指令；
-g：允许远程主机连接主机的转发端口；
-i：指定身份文件；
-l：指定连接远程服务器登录用户名；
-N：不执行远程指令；

-o：指定配置选项；

-p：指定远程服务器上的端口；

-q：静默模式；

-X：开启X11转发功能；

-x：关闭X11转发功能；

-y：开启信任X11转发功能。

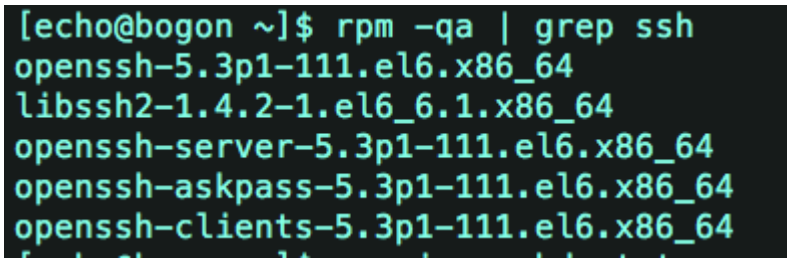
参数

远程主机：指定要连接的远程ssh服务器；

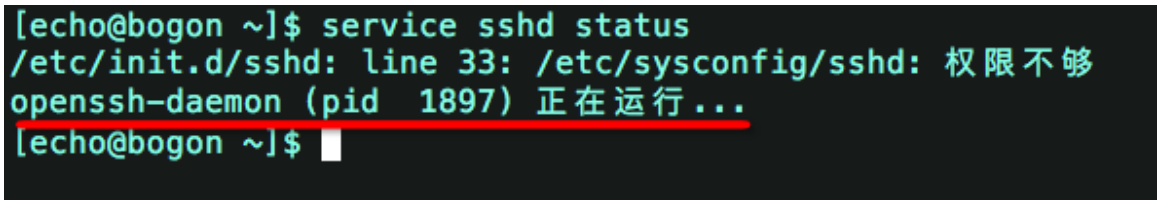
指令：要在远程ssh服务器上执行的指令。

查看SSH是否安装（检查是否装了SSH包）

输入命令：rpm -qa | grep ssh



查看是否运行：service sshd status



安装SSH

yum install ssh

启动SSH

service sshd start

设置开机运行

chkconfig sshd on

安装完以后，一般我们都是通过客户端连接，比如我们当前就是通过 xshell 进行远程连接

2-7 ifconfig

ifconfig命令被用于配置和显示Linux内核中网络接口的网络参数。用ifconfig命令配置的网卡信息，在网卡重启后机器重启后，配置就不存在。要想将上述的配置信息永远的存的电脑里，那就要修改网卡的配置文件了。

语法 ifconfig 参数

参数

add<地址>：设置网络设备IPv6的ip地址；

del<地址>：删除网络设备IPv6的IP地址；

down：关闭指定的网络设备；

io_addr：设置网络设备的I/O地址；

irq：设置网络设备的IRQ；

media<网络媒介类型>：设置网络设备的媒介类型；

mem_start<内存地址>：设置网络设备在主内存所占用的起始地址；

metric<数目>：指定在计算数据包的转送次数时，所要加上的数目；

mtu<字节>：设置网络设备的MTU；

netmask<子网掩码>：设置网络设备的子网掩码；

tunnel<地址>：建立IPv4与IPv6之间的隧道通信地址；

up：启动指定的网络设备；

-broadcast<地址>：将要送往指定地址的数据包当成广播数据包来处理；

-pointopoint<地址>：与指定地址的网络设备建立直接连线，此模式具有保密功能；

-promisc：关闭或启动指定网络设备的promiscuous模式；

IP地址：指定网络设备的IP地址；

网络设备：指定网络设备的名称。

案例：

显示网络设备信息（激活状态的）：

ifconfig

```
[echo@bogon ~]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:98:0E:B6
          inet addr:192.168.1.105  Bcast:192.168.1.255  Mask:255.255.255.
          inet6 addr: fe80::20c:29ff:fe98:eb6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:496 errors:0 dropped:0 overruns:0 frame:0
          TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:51162 (49.9 KiB)  TX bytes:33330 (32.5 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

[echo@bogon ~]$
```

说明:

eth0表示第一块网卡，其中HWaddr表示网卡的物理地址，可以看到目前这个网卡的物理地址(MAC地址)是00:16:3E:00:1E:51。

inet

addr用来表示网卡的IP地址，此网卡的IP地址是10.160.7.81，广播地址Bcast:10.160.15.255，掩码地址Mask:255.255.240.0。

lo是表示主机的回坏地址，这个一般是用来测试一个网络程序，但又不想让局域网或外网的用户能够查看，只能在此台主机上运行和查看所用的网络接口。比如把
httpd服务器的指定到回坏地址，在浏览器输入127.0.0.1就能看到你所架WEB网站了。但只是您能看得到，局域网的其它主机或用户无从知道。

第一行:连接类型:Ethernet(以太网)HWaddr(硬件mac地址)。
第二行:网卡的IP地址、子网、掩码。
第三行:UP(代表网卡开启状态)RUNNING(代表网卡的网线被接上)MULTICAST(支持组播)MTU:1500(最大传输单元):1500字节。
第四、五行:接收、发送数据包情况统计。
第七行:接收、发送数据字节数统计信息。

启动关闭指定网卡:
ifconfig eth0 up　　启动网卡eth0
ifconfig eth0 down　　关闭网卡eth0

备注:ssh登陆linux服务器操作要小心,关闭了就不能开启了

用ifconfig修改MAC地址:
ifconfig eth0 hw ether 00:AA:BB:CC:dd:EE

配置IP地址:
ifconfig eth0 192.168.2.10
ifconfig eth0 192.168.2.10 netmask 255.255.255.0
ifconfig eth0 192.168.2.10 netmask 255.255.255.0 broadcast 192.168.2.255

启用和关闭arp协议:
ifconfig eth0 arp #开启网卡eth0 的arp协议
ifconfig eth0 -arp #关闭网卡eth0 的arp协议

3.服务管理

3-1 chkconfig

chkconfig命令检查、设置系统的各种服务。这是Red Hat公司遵循GPL规则所开发的程序,它可查询操作系统在每一个执行等级中会执行哪些系统服务,其中包括各类常驻服务。谨记chkconfig不是立即自动禁止或激活一个服务,它只是简单的改变了符号连接。

语法 chkconfig [选项]

选项
--
add:增加所指定的系统服务,让chkconfig指令得以管理它,并同时在系统启动的叙述文件内增加相关数据;
--
del:删除所指定的系统服务,不再由chkconfig指令管理,并同时在系统启动的叙述文件内删除相关数据;
--level<运行级别>:指定读系统服务要在哪一个执行等级中开启或关毕。

运行级别列表:
等级0表示:表示关机
等级1表示:单用户模式

等级2表示：无网络连接的多用户命令行模式

等级3表示：有网络连接的多用户命令行模式

等级4表示：不可用

等级5表示：带图形界面的多用户模式

等级6表示：重新启动

使用案例：

chkconfig --list #列出所有的系统服务。

chkconfig --add httpd #增加httpd服务。

chkconfig --del httpd #删除httpd服务。

chkconfig --level httpd 2345 on #设置httpd在运行级别为2、3、4、5的情况下都是on（开启）的状态。

chkconfig --list mysqld #列出mysqld服务设置情况。

chkconfig --level 35 mysqld on #设定mysqld在等级3和5为开机运行服务，--level 35表示操作只在等级3和5执行，on表示启动，off表示关闭。

chkconfig mysqld on #设定mysqld在各等级为on，“各等级”包括2、3、4、5等级。

3-2 service

service命令是Redhat

Linux兼容的发行版中用来控制系统服务的实用工具，它以启动、停止、重新启动和关闭系统服务，还可以显示所有系统服务的当前状态。

语法 service(选项)(参数)

选项

-h：显示帮助信息；

--status-all：显示所服务的状态。

参数

服务名：自动要控制的服务名，即/etc/init.d目录下的脚本文件名；

控制命令：系统服务脚本支持的控制命令(stop 、start、restart、status)。

实例

当修改了主机名、ip地址等信息时，经常需要把网络重启使之生效。

service network status

service network restart

重启mysql
service mysqld status
service mysqld restart

四、小节

2. 课堂练习

3. 课后练习

4. 资料扩展