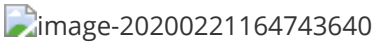
第3天-IP详解及配置

一、ip地址组成

> IP地址由4部分数字组成，每部分数字对应于8位二进制数字，各部分之间用小数点分开 这是点分2进制 如果换算为10进制我们称为点分10进制.
>
> 每个ip地址由两部分组成网络地址(NetID)和主z机地址(HostID).网络地址表示其属于互联网中的哪一个网络，而主机地址则表示其属于该网络中的哪一台主机.

二、ip地址的划分

ip地址划分为五类 为 A,B,C,D,E,如下图



A类地址:范围从0-127，0是保留的并且表示所有IP地址，而127也是保留的地址，并且是用于测试环回用的。因此A类地址的范围其实是从1-126之间。

如：10.0.0.1，第一段号码为网络号码，剩下的三段号码为本地计算机的号码。转换为2进制来说，一个A类IP地址由1字节的网络地址和3字节主机地址组成，网络地址的最高位必须是“0”， 地址范围从0.0.0.1到126.0.0.0。可用的A类网络有126个，每个网络能容纳1亿多个主机（2的24次方的-2主机数目）。

以子网掩码来进行区别：：255.0.0.0
127.0.0.0到127.255.255.255是保留地址，用做循环测试用的

B类地址：范围从128-191，如172.168.1.1，第一和第二段号码为网络号码，剩下的2段号码为本地计算机的号码。转换为2进制来说，一个B类IP地址由2个字节的网络地址和2个字节的主机地址组成，网络地址的最高位必须是“10”，地址范围从128.0.0.0到191.255.255.255。可用的B类网络有16382个，每个网络能容纳6万多个主机 。(2的16次方-2)

以子网掩码来进行区别：255.255.0.0

169.254.0.0到169.254.255.255是保留地址。如果你的IP地址是自动获取IP地址，而你在网络上又没有找到可用的DHCP服务器，这时你将会从169.254.0.0到169.254.255.255中临时获得一个IP地址。

C类地址：范围从192-223，如192.168.1.1，第一，第二，第三段号码为网络号码，剩下的最后一段号码为本地计算机的号码。转换为2进制来说，一个C类IP地址由3字节的网络地址和1字节的主机地址组成，网络地址的最高位必须是“110”。范围从192.0.0.0到223.255.255.255。C类网络可达209万余个，每个网络能容纳254个主机。(2的8次方-2)

以子网掩码来进行区别： 255.255.255.0

D类地址：范围从224-239，D类IP地址第一个字节以“1110”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

224.0.0.0-239.255.255.255 组播地址

E类地址：范围从240-254，以“11110”开始，为将来使用保留。 全零（“0. 0. 0. 0”）地址对应于当前主机。全“1”的IP地址（“255. 255. 255. 255”）是当前子网的广播地 址。

```
240.0.0.0-255.255.255.254 保留地址
```

三、子网掩码

> 就是为了区分ip地址的中的网络号和主机号的

例1：

```
ip地址: 202.197.119.110

若掩码为:255.255.255.0    求网络号和主机号

ip转换为2进制 1100 1010. 1100 0101. 0111 0111. 0110 1110

子网掩码2进制 1111 1111. 1111 1111. 1111 1111. 0000 0000

相与运算      1100 1010. 1100 0101. 0111 0111. 0000 0000    网络号

ip转换为2进制 1100 1010. 1100 0101. 0111 0111. 0110 1110

子网掩码取反  0000 0000. 0000 0000. 0000 0000. 1111 1111

相与运算       0000 0000. 0000 0000. 0000 0000. 0110 1110   主机号
```

例2：

```
ip 202.197.118.110   是否与上一个ip在同一网段?   求网络号，相同则同一网段

ip转换为2进制   1100 1010. 1100 0101. 0111 0110.0110 1110
求得网络号     1100 1010.1100 0101.0111 0110.0000 0000



   网络号   不同，所以不再同一网络中
```

例3:还是上边ip

```
ip地址: 202.197.119.110

若掩码为:255.255.128.0    求网络号和主机号

ip转换为2进制 1100 1010. 1100 0101. 0111 0111. 0110 1110

子网掩码2进制 1111 1111. 1111 1111. 1000 0000. 0000 0000

相与运算      1100 1010. 1100 0101. 0000 0000. 0000 0000    网络号

主机号        0000 0000. 0000 0000. 0111 0111. 0110 1110    主机号


ip 202.197.118.110   是否与上一个ip再统一网段?

ip转换为2进制   1100 1010. 1100 0101. 0111 0110. 0110 1110

求得网络号     1100 1010.1100 0101.0000 0000. 0000 0000
```

同上一个ip在同一个网络中

所以判断两个ip是否在同一网络要看子网掩码的设置

四、私有地址

所谓的私有地址就是在互联网上不使用，而被用在局域网络中的地址

> 在A类地址中，10.0.0.0到10.255.255.255是私有地址
>
> 在B类地址中，172.16.0.0到172.31.255.255是私有地址。
>
> 在C类地址中，192.168.0.0到192.168.255.255是私有地址。

五、可变长子网(vlsm)与超网

> 子网划分是通过增加掩码中“1”的位数来实现的，而超网划分是通过减少掩码中“1”的位数来实现的。获得超网地址的方法也是将超网掩码和IP地址进行按位“与”运算。

无类地址

> 通过前面对子网和超网的介绍，我们看到利用掩码中“1”的位数的增加或减少可以方便地控制网络的规模。在实际应用中许多单位都只需要很少的IP地址，为了方便IP地址的分配和提高IP地址的利用率，1996年因特网组织机构发布了无类别域间路由CIDR （ Classless Interdomain Routing ）。
>
> CIDR去掉了A类地址、B类地址和C类地址的概念，采用了无类地址的概念，不再由地址的前几个比特来预先定义网络类别。每一个地址仅仅包含网络号部分和主机号部分。

六、实战

1、熟记IP地址分类

2、熟练子网掩码的用法

七、mac地址

查看mac地址

```
[root@qfedu.com ~]#  ifconfig

[root@qfedu.com ~]#  ip  a

[root@qfedu.com ~]#  arping  172.16.70.250

[root@qfedu.com ~]#  arping -I enp0s25 10.18.44.208
ARPING 10.18.44.208 from 10.18.44.196 enp0s25

Unicast reply from 10.18.44.208 [00:21:CC:C1:42:4B]  1.113ms

Unicast reply from 10.18.44.208 [00:21:CC:C1:42:4B]  0.975ms
```

查询mac地址和ip地址的对应关系

arp表

```
[root@qfedu.com ~]#  arp  -a
```

八、Linux网络管理

1、查看ip地址

```
[root@qfedu.com ~][root@qfedu.com ~]#  ifconfig eth0   //单独查看eth0

[root@qfedu.com ~][root@qfedu.com ~]#  ifconfig   //查看所有网卡

[root@qfedu.com ~][root@qfedu.com ~]#  ip a        //查看所有网卡

[root@qfedu.com ~][root@qfedu.com ~]#  ip  a s eth0   //单独查看eth0

[root@qfedu.com ~][root@qfedu.com ~]#  ip  a l eth0
```

2、配置IP

```
[root@qfedu.com ~][root@qfedu.com ~]#  ifconfig  eth0  192.168.2.250/24    //会覆盖旧的IP
[root@qfedu.com ~][root@qfedu.com ~]#  ifconfig  eth0:0  192.168.2.251/24
子网掩码可以不写

[root@qfedu.com ~][root@qfedu.com ~]#  ip  addr  add  192.168.2.250/24  dev eth0
[root@qfedu.com ~][root@qfedu.com ~]#  ip a a 192.168.2.250/24 dev eth0
[root@qfedu.com ~][root@qfedu.com ~]#  ip a d 192.168.2.8/24 dev enp0s25
子网掩码必须写

add 添加IP 简写成a
del  删除IP 简写成d
```


启动网卡

```
[root@qfedu.com ~][root@qfedu.com ~]#  ifconfig eth0  up
[root@qfedu.com ~][root@qfedu.com ~]#  ifup  eth0
```

关闭网卡

```
[root@qfedu.com ~][root@qfedu.com ~]#  ifconfig eth0 down
[root@qfedu.com ~][root@qfedu.com ~]#  ifdown eth0
```

配置文件

静态IP：

```
[root@qfedu.com ~]# vim  /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

NAME="System eth0"    //名称  可以不存在

BOOTPROTO=none      //（none或static 静态获取 ）（dhcp 动态获取IP）
```

```
NM_CONTROLLED=no    //关闭NetworkManager

ONBOOT=yes           //开机启动

TYPE=Ethernet          // 以太网类型

HWADDR=00:0c:29:8e:a5:d3  //MAC地址

IPADDR=172.16.80.252    //IP地址

NETMASK=255.255.0.0    //子网掩码

PREFIX=24             //子网掩码

NETWORK=172.16.0.0    //网络

GATEWAY=172.16.0.1     //网关

DNS1=172.16.0.1        //domain name server域名服务器

DNS2=114.114.114.114   //第2台DNS服务器
```

动态IP：

```
[root@qfedu.com ~]# vim  /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0

NAME="System eth0"     //名称  可以不存在

BOOTPROTO=dhcp       //（none或static 静态获取 ）（dhcp 动态获取IP）

ONBOOT=yes           //开机启动

TYPE=Ethernet          // 以太网类型
```


重启网络服务：配置文件修改后必须重起网络服务

```
[root@qfedu.com ~]# systemctl restart network  //rhel7

[root@qfedu.com ~]# /etc/init.d/network restart  //rhel5/6

[root@qfedu.com ~]# service  network  restart   //rhel5/6
```

九、网络测试工具

1、ping命令

> 用来测试主机之间网络的连通性。执行ping指令会使用ICMP传输协议，发出要求回应的信息，若远端主机的网络功能没有问题，就会回应该信息，因而得知该主机运作正常。

用法

> ping命令运行在命令提示符终端，用法为：“ping 参数 目标主机”。其中参数为零到多个，目标主机可以是IP或者域名。

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。
>
> ping 192.168.1.9 开始；ctrl + c 停止
>
> ping命令通过ICMP（Internet控制消息协议）工作；ping可以用来测试本机与目标主机是否联通、联通速度如何、稳定性如何。

ping参数详解

> 参数 详解
>
> -a Audible ping.
>
> -A 自适应ping，根据ping包往返时间确定ping的速度；
>
> -b 允许ping一个广播地址；
>
> -B 不允许ping改变包头的源地址；
>
> -c count ping指定次数后停止ping；
>
> -d 使用Socket的SO_DEBUG功能；
>
> -F flow_label 为ping回显请求分配一个20位的“flow label”，如果未设置，内核会为ping随机分配；
>
> -f 极限检测，快速连续ping一台主机，ping的速度达到100次每秒；
>
> -i interval 设定间隔几秒发送一个ping包，默认一秒ping一次；
>
> -I interface 指定网卡接口、或指定的本机地址送出数据包；
>
> -l preload 设置在送出要求信息之前，先行发出的数据包；

-L 抑制组播报文回送，只适用于ping的目标为一个组播地址

-n　不要将ip地址转换成主机名；

-p pattern 指定填充ping数据包的十六进制内容，在诊断与数据有关的网络错误时这个选项就非常有用，如：“-p ff”；

-q　不显示任何传送封包的信息，只显示最后的结果

-Q tos 设置Qos(Quality of Service)，它是ICMP数据报相关位；可以是十进制或十六进制数，详见rfc1349和rfc2474文档；

-R　记录ping的路由过程(IPv4 only)；

注意：由于IP头的限制，最多只能记录9个路由，其他会被忽略；

-r 忽略正常的路由表，直接将数据包送到远端主机上，通常是查看本机的网络接口是否有问题；如果主机不直接连接的网络上，则返回一个错误。

-S sndbuf　Set socket sndbuf. If not specified, it is selected to buffer not more than one packet.

-s packetsize 指定每次ping发送的数据字节数，默认为“56字节”+“28字节”的ICMP头，一共是84字节；

包头+内容不能大于65535，所以最大值为65507（linux:65507, windows:65500）；

-t ttl 设置TTL(Time To Live)为指定的值。该字段指定IP包被路由器丢弃之前允许通过的最大网段数；

-T timestamp_option　设置IP timestamp选项,可以是下面的任何一个：

'tsonly' (only timestamps)

'tsandaddr' (timestamps and addresses)

'tsprespec host1 [host2 [host3]]' (timestamp prespecified hops).

-M hint　设置MTU（最大传输单元）分片策略。

可设置为：

'do'：禁止分片，即使包被丢弃；

'want'：当包过大时分片；

'dont'：不设置分片标志（DF flag）；

-m mark 设置mark；

-v 使ping处于verbose方式，它要ping命令除了打印ECHO-RESPONSE数据包之外，还打印其它所有返回的ICMP数据包；

-U　Print full user-to-user latency (the old behaviour).

Normally ping prints network round trip time, which can be different f.e. due to DNS failures.

-W timeout　以毫秒为单位设置ping的超时时间；

-w deadline　deadline；

2、traceroute

> 通过traceroute我们可以知道信息从你的计算机到互联网另一端的主机是走的什么路径。当然每次数据包由某一同样的出发点（source）到达某一同样的目的地(destination)走的路径可能会不一样，但基本上来说大部分时候所走的路由是相同的。linux系统中，我们称之为traceroute,在MS Windows中为tracert。 traceroute通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。一条路径上的每个设备traceroute要测3次。输出结果中包括每次测试的时间(ms)和设备的名称（如有的话）及其IP地址。

在大多数情况下，我们会在linux主机系统下，直接执行命令行：

```
[root@qfedu.com ~]# traceroute hostname
```

如果执行过程中没有traceroute 命令，可通过
yum -y install traceroute 命令安装下（root权限在线安装）

1.命令格式：

```
[root@qfedu.com ~]# traceroute [参数] [主机]
```

2.命令功能：

traceroute指令让你追踪网络数据包的路由途径，预设数据包大小是40Bytes，用户可另行设置。

具体参数格式：

```
[root@qfedu.com ~]#traceroute [-dFlnrvx][-f<存活数值>][-g<网关>...][-i<网络界面>][-m<存活数值>][-p<通信端口>][-s<来源地址>][-t<服务类型>][-w<超时秒数>][主机名称或IP地址][数据包大小]
```


3.命令参数：

-d 使用Socket层级的排错功能。

-f 设置第一个检测数据包的存活数值TTL的大小。

-F 设置勿离断位。

-g 设置来源路由网关，最多可设置8个。

-i 使用指定的网络界面送出数据包。

-I 使用ICMP回应取代UDP资料信息。

-m 设置检测数据包的最大存活数值TTL的大小。

-n 直接使用IP地址而非主机名称。

-p 设置UDP传输协议的通信端口。

-r 忽略普通的Routing Table，直接将数据包送到远端主机上。

-s 设置本地主机送出数据包的IP地址。

-t 设置检测数据包的TOS数值。

-v 详细显示指令的执行过程。

-w 设置等待远端主机回报的时间。

-x 开启或关闭数据包的正确性检验。

4.使用实例

实例1：traceroute 用法简单、最常用的用法

命令：

```
[root@qfedu.com ~]#traceroute www.qfedu.com
```

说明：

> 记录按序列号从1开始，每个纪录就是一跳 ，每跳表示一个网关，我们看到每行有三个时间，单位是 ms，其实就是-q的默认参数。探测数据包向每个网关发送三个数据包后，网关响应后返回的时间；如果用 traceroute -q 4 www.qfedu.com ，表示向每个网关发送4个数据包。
>
> 有时我们traceroute 一台主机时，会看到有一些行是以星号表示的。出现这样的情况，可能是防火墙封掉了ICMP的返回信息，所以我们得不到什么相关的数据包返回数据。
>
> 有时我们在某一网关处延时比较长，有可能是某台网关比较阻塞，也可能是物理设备本身的原因。当然如果某台DNS出现问题时，不能解析主机名、域名时，也会 有延时长的现象；您可以加-n 参数来避免DNS解析，以IP格式输出数据。
>
> 如果在局域网中的不同网段之间，我们可以通过traceroute 来排查问题所在，是主机的问题还是网关的问题。如果我们通过远程来访问某台服务器遇到问题时，我们用到traceroute 追踪数据包所经过的网关，提交IDC服务商，也有助于解决问题；但目前看来在国内解决这样的问题是比较困难的，就是我们发现问题所在，IDC服务商也不可能帮助我们解决。

实例2：跳数设置

命令：

```
[root@qfedu.com ~]#traceroute -m 10 www.baidu.com
```


实例3：显示IP地址，不查主机名

命令：

```
[root@qfedu.com ~]#traceroute -n www.baidu.com
```

实例4：探测包使用的基本UDP端口设置6888

命令：

```
[root@qfedu.com ~]#traceroute -p 6888 www.baidu.com
```

实例5：把探测包的个数设置为值4

命令：

```
[root@qfedu.com ~]#traceroute -q 4 www.baidu.com
```

实例6：绕过正常的路由表，直接发送到网络相连的主机

命令：

```
[root@qfedu.com ~]# traceroute -r www.baidu.com
```

报的是网络不可达。

实例7：把对外发探测包的等待响应时间设置为3秒

命令：

```
[root@qfedu.com ~]#traceroute -w 3 www.baidu.com
```

Traceroute的工作原理

> Traceroute程序的设计是利用ICMP及IP header的TTL（Time To Live）栏位（field）。首先，traceroute送出一个TTL是1的IP datagram（其实，每次送出的为3个40字节的包，包括源地址，目的地址和包发出的时间标签）到目的地，当路径上的第一个路由器（router）收到这个datagram时，它将TTL减1。此时，TTL变为0了，所以该路由器会将此datagram丢掉，并送回一个「ICMP time exceeded」消息（包括发IP包的源地址，IP包的所有内容及路由器的IP地址），traceroute 收到这个消息后，便知道这个路由器存在于这个路径上，接着traceroute 再送出另一个TTL是2 的datagram，发现第2 个路由器..... traceroute 每次将送出的datagram的TTL 加1来发现另一个路由器，这个重复的动作一直持续到某个datagram 抵达目的地。当datagram到达目的地后，该主机并不会送回ICMP time exceeded消息，因为它已是目的地了，那么traceroute如何得知目的地到达了呢？
>
> Traceroute在送出UDP datagrams到目的地时，它所选择送达的port number 是一个一般应用程序都不会用的号码（30000 以上），所以当此UDP datagram 到达目的地后该主机会送回一个「ICMP port unreachable」的消息，而当traceroute 收到这个消息时，便知道目的地已经到达了。所以traceroute 在Server端也是没有所谓的Daemon 程式。
>
> Traceroute提取发 ICMP TTL到期消息设备的IP地址并作域名解析。每次 ，Traceroute都打印出一系列数据,包括所经过的路由设备的域名及 IP地址,三个包每次来回所花时间。

十、实战

1、配置IP地址并实现网络通信

2、测试ping命令常用选项

3、测试tracerote常用选项