

运维网络基础

运维网络基础

1.什么是网络?

2. 网络设备说明介绍

3. 网络层次结构

4. 数据包封装与解封装

5. TCP/IP模型 (4层模型)

6. IP地址

7. 子网掩码

8. 网关

9. 抓包方式

10. Linux常用网络命令

1. 什么是网络?

1

2 所谓网络，就是通过一定的形式连接起来的物体，物体与物体之间可以实现通信。

3 用什么连接：

4 网线

5 网线分类：五类线 超五类 六类线(千兆) 按箱
子305米

6 水晶头 橙白 橙 绿白 蓝 蓝白 绿 棕白 棕
7 568B线序(568A线序)
8 8芯线: 4芯 1236芯 用来传输数据 其他4芯没
用(额外供电 反向供电 POE供电)
9 传输距离100米(超过100米需要加信号放大器 交
换机 HUB)
10 光纤 千兆万兆
11 多模光纤 传输距离近 2公里
12 单模光纤 传输距离远 120公里
13 wifi
14 物体于物体:
15 计算机-计算机
16 计算机-服务器
17 服务器-服务器
18 计算机-交换机
19 计算机-路由器
20 交换机-交换机
21 路由器-路由器
22
23 物联网: 所有的物体都是由网络进行互通互联
24 ip不够用
25 #网络的重要性
26
27 所有的系统都有网络!
28 我们的生活已经离不开网络。
29 运维生涯50%的生产故障都是网络故障!
30

1. 如何通过网络实现多台主机之间的通讯

1
2 1)在两台主机之间需要有传输介质(网线、光纤、无线等)

3
4 2)在两台主机上面需要有网卡设备
5 网卡： 全球唯一的地址(MAC) 类似家的位置
6
7 在发送信息时： 将二进制（数字信号）信息转换为高低
8 电压（电信号） #调至过程
9 在接收信息时： 将高低电压（电信号）信息转换为二进
10 制数（数字信号） #解调过程
11 3)在进行数据传输之前，需要协商网络传输速率。
12
13 网卡速度参数 100Mbps==100M bit 每秒==每秒钟
14 传输多少个bit (0或1)
15 1M=1000k 100M=100000k
16
17 网络传输数据单位： 比特 bit 1bit=1/8byte
18 磁盘存储数据单位： 字节 byte 1byte=8bit
19 网卡的100Mbps同样是以bit/s来定义的 所以100Mb/s=
20 100000KByte/s=(100000/8)KByte/s=12500KByte/s
21 在理论上1秒钟可以传输12.5MB的速据 考虑到 干扰的因素
22 每秒传输只要超过10MB就是正常了 现在出现了1000Mbps
23 的网卡那么速度就是100MB/s
24 K是千 M是兆 G是吉咖 T是太拉
25
26 1Byte(字节)=8bit(位)
27
28 1KB=1024Byte(字节)
29 1MB=1024KB
30 1024MB=1GB

30
31 1024GB=1TB
32
33 真实的运营商下载带宽：ADSL拨号 用户名和密码 非对称式网络 上传和下载带宽不一样 家用
34 重启路由器重新获取新的公网IP地址
35 2M 4M
36 6M 8M
37 企业专线：对称式网络 配置公网IP地址 上传和下载相同 价格翻好几倍 10MB 4-8万 运营商不同

2. 网络设备说明介绍

*1. 什么是交换机*3

1
2 实现一个网络内多台主机之间的通讯
3
4 #如何利用交换机实现通讯
5
6 1. 在数据前面设置目标地址和源地址，目标地址和源地址用mac地址进行标识
7 mac称为物理地址，每块网卡上都有的一个标识身份信息的
8 mac地址全球唯一，不能进行修改，mac地址用16进制标识
9
10 2. 在网络通讯初期，会利用广播方式进行发送数据包，在通讯的过程，数据包的发送一定是有去有回的。
11 在一个交换网路中，如果产生了大量广播数据包时会产生广播风暴，影响主机性能，这样的问题称为广播风暴问题
12

```
13 #解决广播风暴问题思路:  
14  
15     减少广播产生数量，将一个大的交换网络切割为几个小的交换网络（局域网，广播域）  
16  
17 #交换机的种类  
18  
19     傻瓜交换机（TP-link/Dlink/水星...）  
20     4口 8口 12口 16口 24口 48口  
21     程控交换机（存储程序控制交换机，配置管理，思科、华为、华三、锐捷、中兴、瑞斯康达）  
22     二层交换 支持数据转发 vlan隔离端口  
23     三层交换 功能比较多 DHCP ACL访问控制列表 支持路由器功能  
24 OSI七层模型
```



思科

交换机硬件设备

2. 什么是路由器

- 1
- 2 实现不同局域网之间主机通讯，可以隔离广播风暴（路由不同的接口连接不同广播域）
- 3

4 路由类似于现实生活中从**A**地去往**B**地可能需要先步行，在坐车，在做飞机才能到达**B**地，这样的整个过程在网络中对应数据的传递过程就称为路由。因此一个数据信息跨越不同的网段传递到目的地址，就可以把传递数据的过程称为路由，也可以看做每条传递数据的路径。

5

6 1) 需要有身份标识信息：**ip地址**

7 逻辑地址（可以改变的地址/? ? ? ） 利用**10**进制方式进行显示

8 **IP**地址由两部分组成： 交换网络标识信息+主机地址标识信息==网段地址+主机地址

9 192.168.13 网段 1-254

10 主机地址

11 10.0.0 网段 1-254 主机地址

12 昌平区 网段 xx地址

13 192.168.11.x

14 海淀区 网段 xx地址

15 192.168.10.x

16 内网卡---交换机

17 192.168.11.0/24(192.168.11.1~192.168.11.254)

18 外网卡---运营商 IP : 221.218.210.53

19

20 查公网**ip**的方法:

21 windows, 打开浏览器, 访问百度, 搜**IP**即可

22 linux: curl ifconfig.me ip.sb

23

24 高级路由器还有上网行为管理器和防火墙功能

25 论坛: 鸿鹄论坛(网络工程师)

26

27 2) 路由实现数据传输通讯时，会根据路由表信息进行数据包路由

24 实现不同网段之间通讯需要经过一条必经之路，这条路
称为网关

25

26 经过了多少跳 经过了多少个路由器

27 下一跳 下一个路由器的接口 下一个路由器IP

28 我们到百度中间经过了多少跳？ 经过了多少个路由器。

29

30 -----

31 配置通过一个路由器实现让不同网段通信

32 Router>

33 Router>?

34 Exec commands:

35 <1-99> Session number to resume

36 connect Open a terminal connection

37 disable Turn off privileged commands

38 disconnect Disconnect an existing
network connection

39 enable Turn on privileged commands

40 exit Exit from the EXEC

41 logout Exit from the EXEC

42 ping Send echo messages

43 resume Resume an active network
connection

44 show Show running system
information

45 ssh Open a secure shell client
connection

46 telnet Open a telnet connection

47 terminal Set terminal line parameters

48 traceroute Trace route to destination

49 Router>enable # 进入特权模式 可以简写en

50 Router#

```
51
52 Router#show running-config # 查看当前路由器所
53 有的配置
53 Router# config t # 进入到配置模式
54 Router(config)#interface fa0/0 # 可以简写
55 int fa0/0 进入到这个接口
55 Router(config-if)#
56 Router(config-if)#ip address 10.0.0.1
57 255.255.255.0 # 配置IP地址为10.0.0.1
57 Router(config-if)#
58 Router(config-if)#no shutdown # 开启此端口
59 Router(config-if)#int fa0/1 # 切换到
60 fa0/1接口
60 Router(config-if)#
61
62 Router(config-if)#ip add 116.63.0.1
63 255.255.255.0
63 Router(config-if)#no shut
64
65 Router#
66 Router#show ip route
67 10.0.0.0/24 is subnetted, 1 subnets
68 C 10.0.0.0 is directly connected,
69 FastEthernet0/0
70 116.0.0.0/24 is subnetted, 1 subnets
71 C 116.63.0.0 is directly connected,
72 FastEthernet0/1
73
74 面试题：如何让不同的网段进行通信？
75 中间加个路由器。
76 -----
77 -----
```

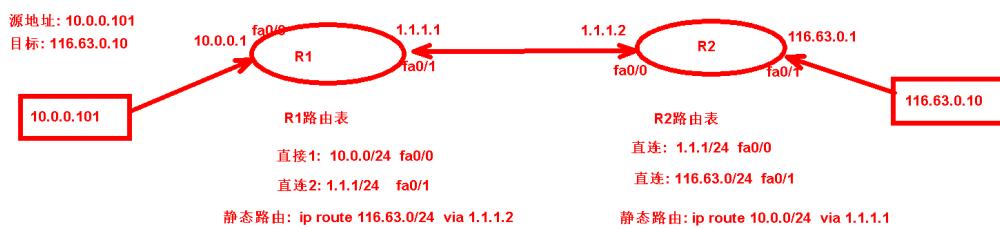
```
76 两个路由器配置：  
77 R1路由器  
78 Router>enable  
79 Router#  
80 Router#config t  
81 Enter configuration commands, one per line.  
End with CNTL/Z.  
82 Router(config)#int fa0/0  
83 Router(config-if)#ip add 10.0.0.1  
255.255.255.0  
84 Router(config-if)#no shut  
85 Router(config-if)#no shutdown  
86  
87 Router(config-if)#int fa0/1  
88 Router(config-if)#ip add 1.1.1.1  
255.255.255.0  
89 Router(config-if)#no shut  
90  
91  
92 查看R1路由器路由表  
93 Router#show ip route  
94      1.0.0.0/24 is subnetted, 1 subnets  
95 C          1.1.1.0 is directly connected,  
FastEthernet0/1  
96      10.0.0.0/24 is subnetted, 1 subnets  
97 C          10.0.0.0 is directly connected,  
FastEthernet0/0  
98 Router#  
99 Router(config)#ip route 116.63.0.0  
255.255.255.0 1.1.1.2  
100  
101  
102
```

```

103 R2路由器配置
104 Router(config)#int fa0/0
105 Router(config-if)#ip add 1.1.1.2
    255.255.255.0
106 Router(config-if)#no shut
107 Router(config-if)#no shutdown
108
109 Router(config-if)#int fa0/1
110 Router(config-if)#ip add 116.63.0.1
    255.255.255.0
111 Router(config-if)#no shut
112 Router(config)#ip route 10.0.0.0
    255.255.255.0 1.1.1.1
113
114
115 -----
-----
```

116

静态路由 手动指定路由信息到目标地址



三个路由器配置:



- 1 修改R2路由器配置：
- 2 Router(config)#int fa0/1
- 3 Router(config-if)#no ip address # 删除接口的IP地址
- 4 Router(config-if)#ip add 2.2.2.1
255.255.255.0
- 5 Router(config-if)#no shut
- 6 Router(config)#ip route 116.63.0.0
255.255.255.0 2.2.2.2
- 7
- 8
- 9
- 10 R3路由器配置
- 11 Router>enable
- 12 Router#config t
- 13 Enter configuration commands, one per line.
End with CNTL/Z.
- 14 Router(config)#int fa0/0
- 15 Router(config-if)#ip add 2.2.2.2
255.255.255.0
- 16 Router(config-if)#no shut
- 17 Router(config-if)#int fa0/1
- 18 Router(config-if)#ip add 116.63.0.1
255.255.255.0
- 19 Router(config-if)#no shut

```
20 Router(config)#ip route 10.0.0.0  
255.255.255.0 2.2.2.1
```

```
21
```

1 动态路由(路由自动学习过程)
2 RIP OSPF EIGRP ISIS BGP
3 来老男孩学习(协议 RIP)
4 R1 张前龙： 金融 厨师 将我会的技能告诉相邻的同桌(路由器)我会什么 经理 PS 艺术 直播
5 R2 王亚楠： 经理 PS 自动从R1路由器学习了金融和厨师技能，告诉相邻的路由我会什么 经理 PS 金融 厨师 艺术直播
6 R3 黄雅萍 艺术 直播 自动从R2路由器学习到了 经理 PS 金融 厨师 告诉相邻的路由器我会什么 艺术 直播
7
8
9
10 R1路由器配置：
11 第一步：启动协议
12 Router#config t
13 Enter configuration commands, one per line.
End with CNTL/Z.
14 Router(config)#route rip # 进入到rip协议
15
16 第二步：宣告自己的网段

```
17 Router(config-router)#network 10.0.0.0
18 Router(config-router)#network 1.1.1.0
19
20 R2路由器配置
21
22 Router#config t
23 Enter configuration commands, one per line.
  End with CNTL/Z.
24 Router(config)#route rip
25 Router(config-router)#network 1.1.1.0
26 Router(config-router)#network 2.2.2.0
27
28 R3路由器配置
29 Router#config t
30 Enter configuration commands, one per line.
  End with CNTL/Z.
31 Router(config)#route rip
32 Router(config-router)#network 2.2.2.0
33 Router(config-router)#network 116.63.0.0
```

3. 网络层次结构

1. 网络拓扑

1

2 网络层次结构

3 核心层：主要部署路由器设备，用于连接外网线路，还要具备冗余能力

4 汇聚层：主要部署三层交换设备，用于相应安全访问控制 进行链路汇聚

5 接入层：主要部署二层交换设备，用于终端设备接入

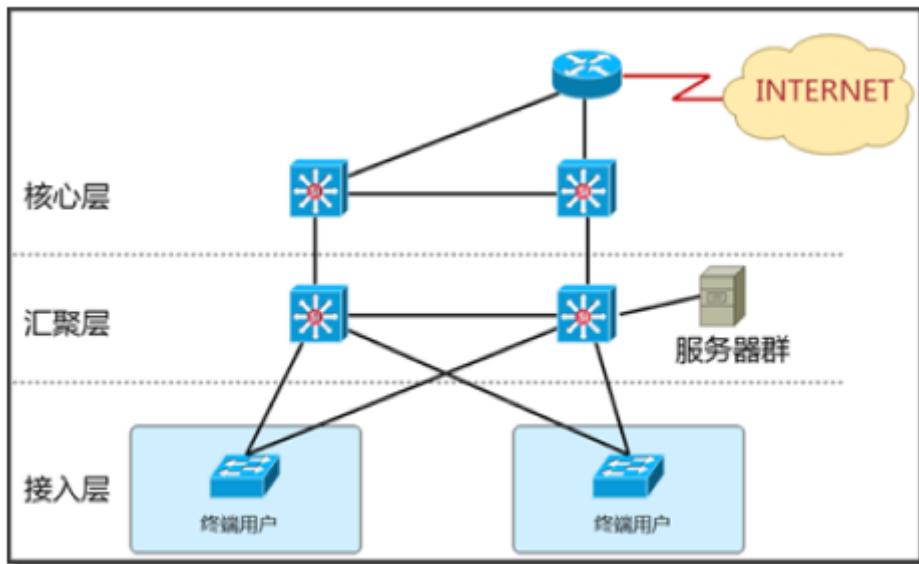
6

7 一层交换机：只支持物理层协议。

8 二层交换机：支持物理层和数据链路层协议。

9 三层交换机：支持物理层，数据链路层及网络层协议。

10



基本网络层次

划分标准示意图

2. 网络类型

1

2 局域网：本地私有的一个网络范围。规模较大的局域网，
也会称为园区网。

3 教室 家庭 公司内 校园

4 公网：全球任意一个可以上网的地方都可以直接访问到

5
6 城域网：网络的覆盖面积达到了一个城市，就可以称为城
域网。

7
8 广域网：覆盖面积 达到了全国或全球，就称为广域网，
全球最大的广域网就是Internet互联网。

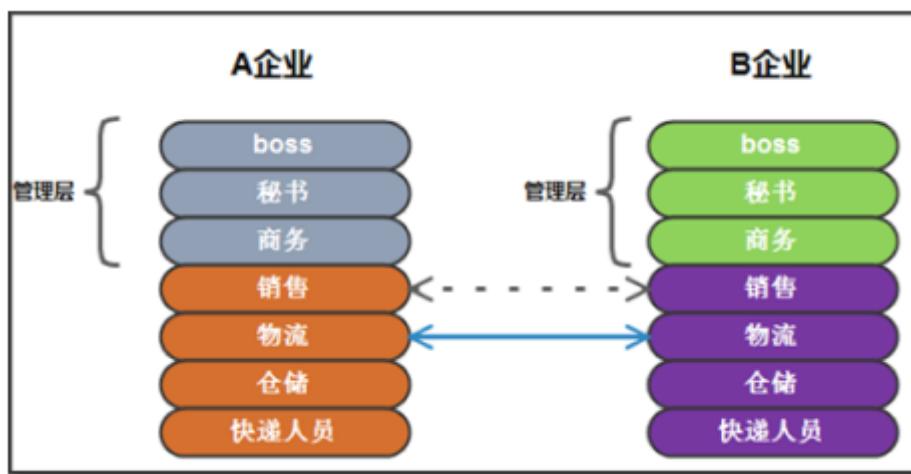
9

*3. 网络层次模型 (OSI7层模型) *

1

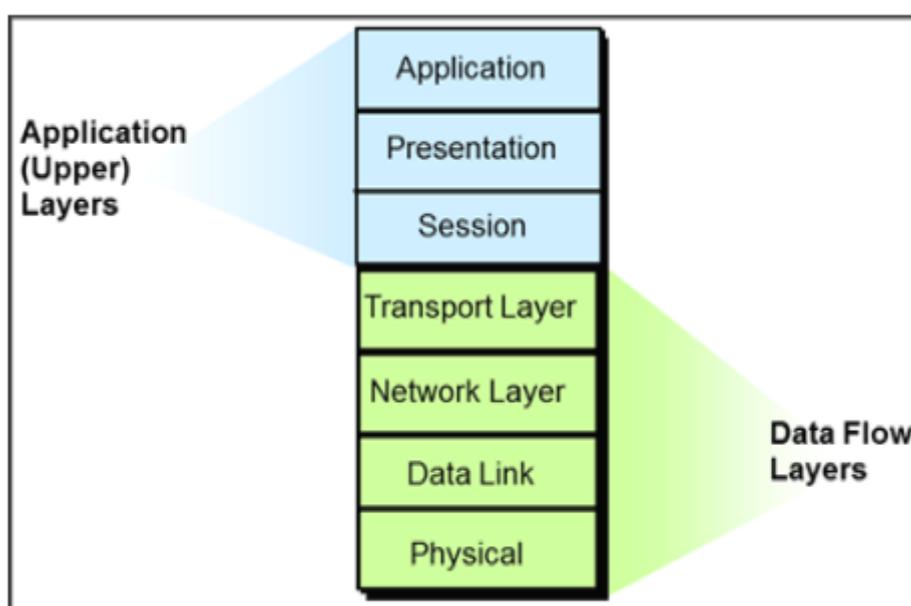
2 OSI是Open System Interconnection的缩写，意为开放式系统互联。国际标准化组织（ISO）制定了OSI模型，该模型定义了不同计算机互联的标准，是设计和描述计算机网络通信的基本框架。OSI模型把网络通信的工作分为7层，分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

OSI七层模型功能介绍



OSI 7层

模型形象比喻示意图

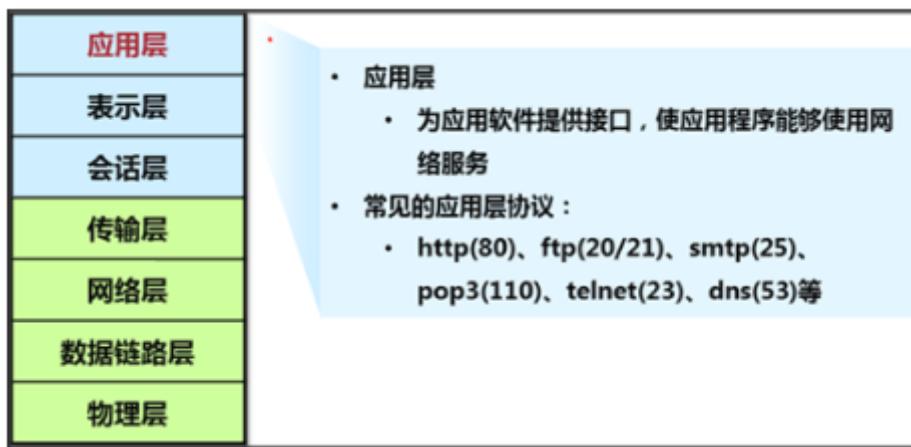


模型结构示意图

4. OSI七层模型详解

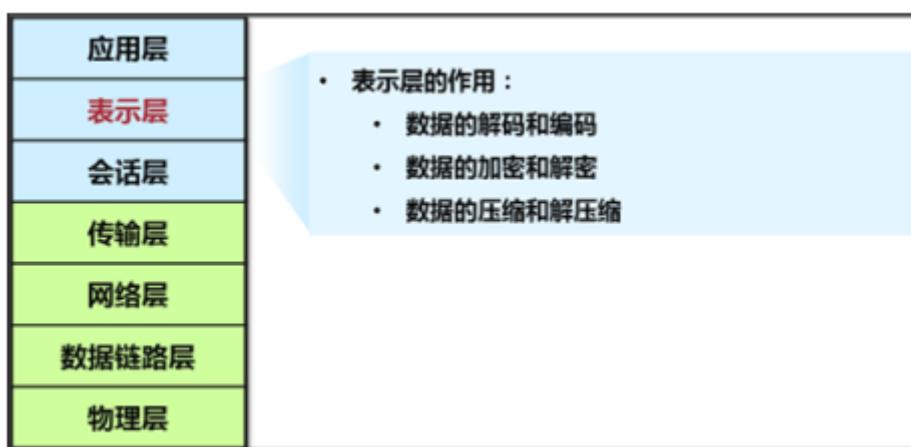
应用层

面试题说一下七层模型都有哪七层？

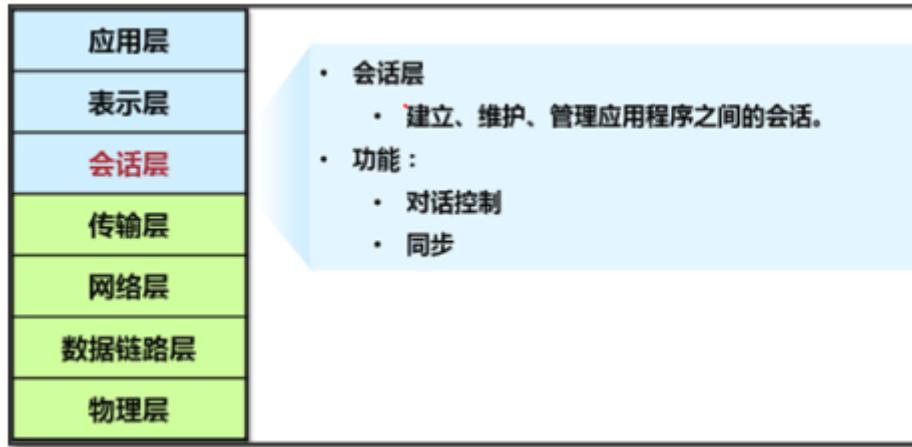


- 1
- 2 主要就是提供应用程序可以接入网络接口，并根据程序的不同对应不同的接口协议。
- 3

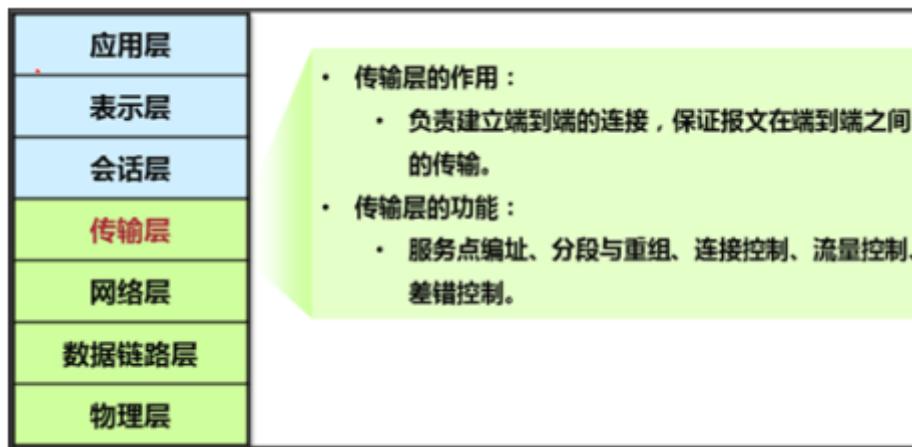
表示层



会话层

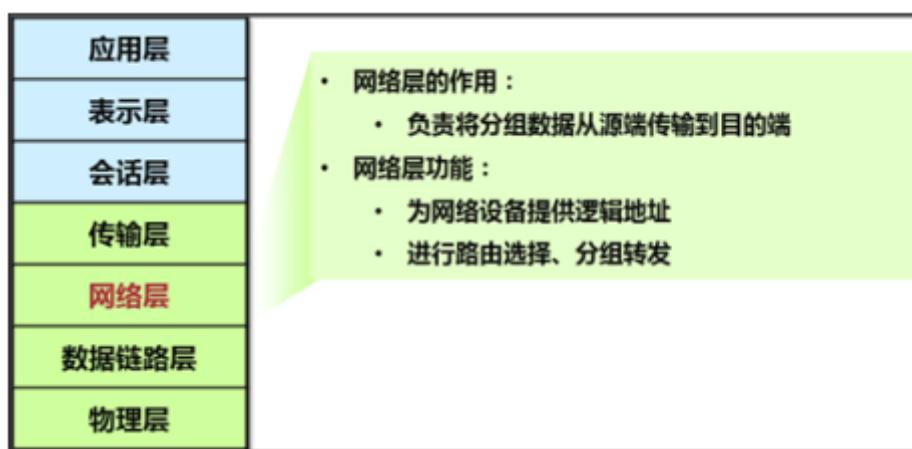


传输层



- 1
- 2 负责网络中端到端的连接（TCP、UDP）。
- 3

网络层

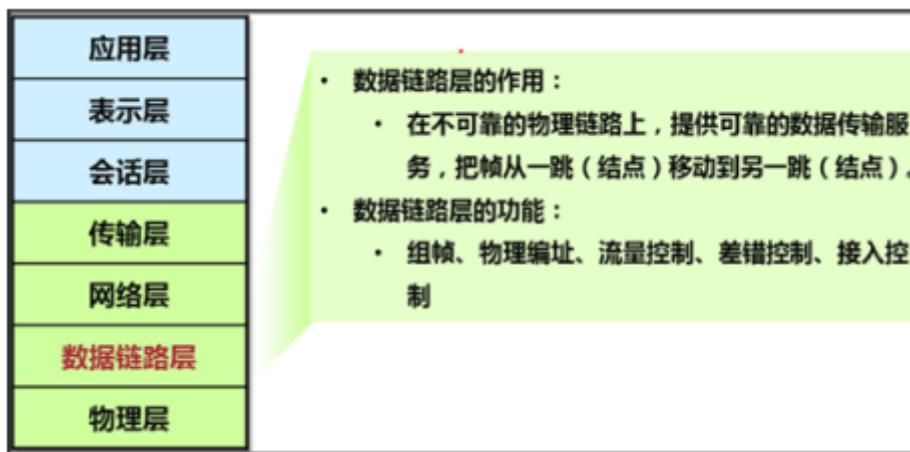


1

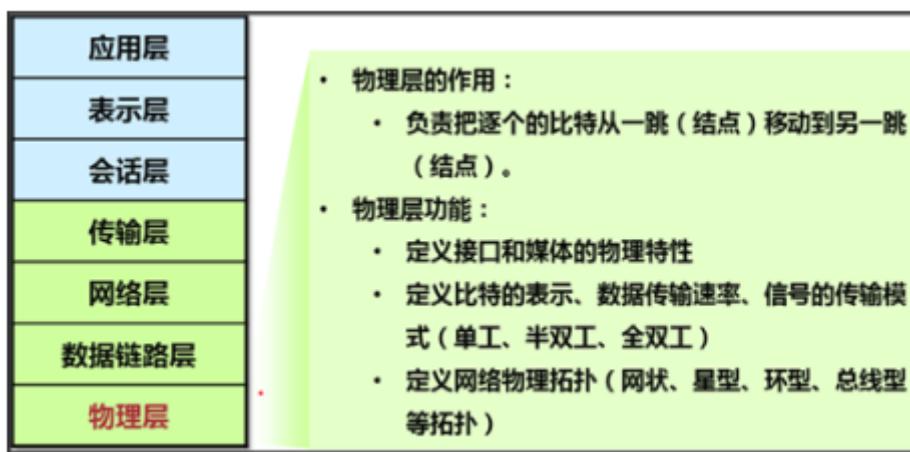
2 网络层的主要作用就是路由和寻址，主要接触到的是IP协议，即IP地址。

3

数据链路层



物理层



1

2 Layer1物理层：物理层标准规定了信号、连接器和电缆要求、接口类型、线缆类型、设备（集线器hub）。

3

4 单工：（广播电台）通讯时候。只有一方作为发送方，另一方作为接受方

5

6 半双工：（对讲机）通讯的某一时刻，只有一方作为发送方，另一方作为接受方，通讯时刻发生转变，发送方可以变为接收方，接收方可以变为发送方

7

8 全双工：（电话）同一时刻，双方皆可以是发送方，又可以是接收方

9

4. 数据包封装与解封装

封装

1

2 封装过程：由上至下进行封装

3 应用层、表示层、会话层 PDU 数据

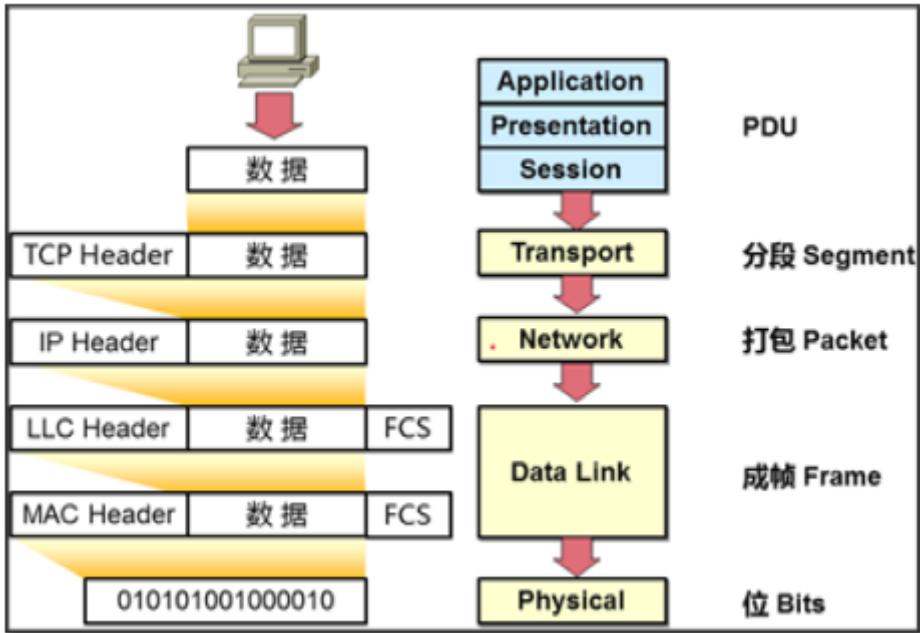
4 传输层：分段 TCP协议

5 网络层：打包 TCP协议+IP地址

6 数据链路层：成帧 TCP协议+IP地址+MAC地址

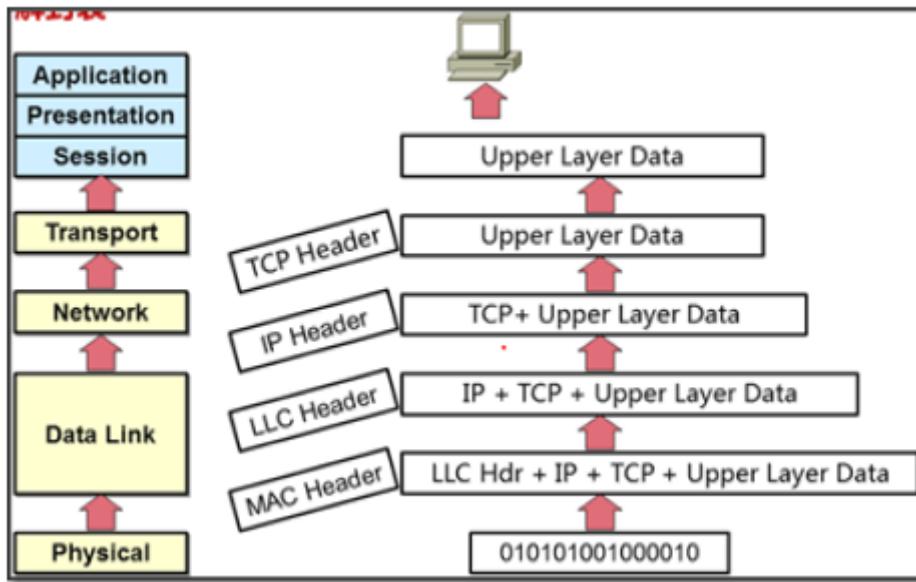
7 物理层：位 数据成为比特

8



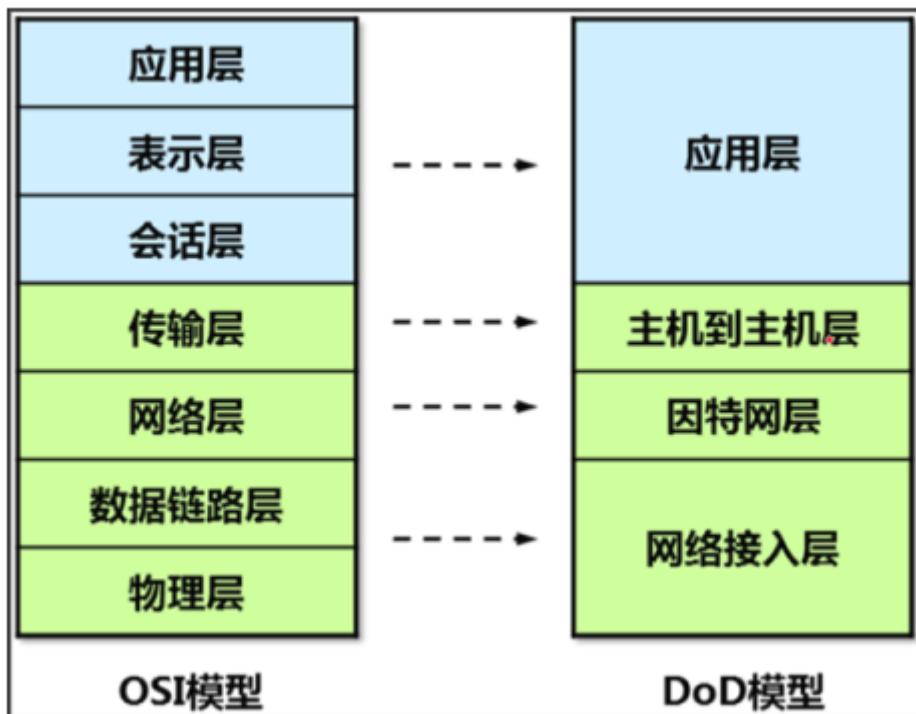
解封装

- 1
- 2 拆包过程：由下至上进行拆包
- 3 物理层：位 比特
- 4 数据链路层：查看**MAC地址**
- 5 网络层：查看**IP地址**
- 6 传输层：查看**TCP协议**
- 7 前三层：数据内容
- 8
- 9 不知名端口：1024以上的端口称为不知名端口
- 10 `cat /proc/sys/net/ipv4/ip_local_port_range`
- 11

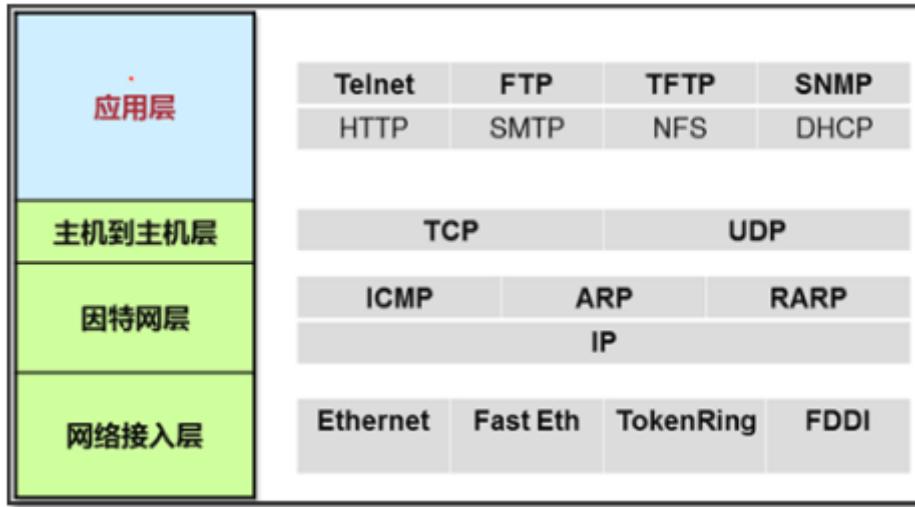


5. TCP/IP模型 (4层模型)

1. OSI7层模型与TCP/IP模型 (DOD) 对应关系



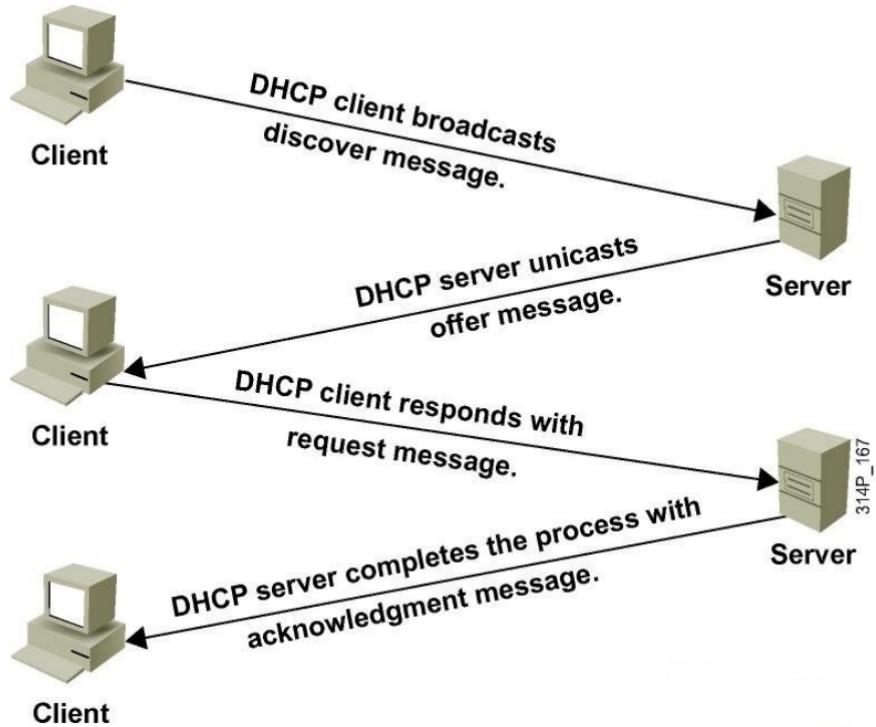
2. TCP/IP协议簇相关协议汇总



3. 应用层协议介绍

- | | | |
|----|--|--------------------------------|
| 1 | 面试题：面试官问 ssh 默认端口 http 默认端口？ | |
| 2 | FTP 21 | 明文协议，文件传输协议，基于TCP |
| 3 | TFTP 69 | 简单文件传输协议，基于UDP |
| 4 | SSH 22 | 安全外壳协议，远程连接，加密 |
| 5 | Telnet 23 | 明文协议，远程连接 |
| 6 | SNMP 161/162 | 简单网络管理协议，基于UDP |
| 7 | SMTP 25 | 简单邮件传输协议，基于TCP |
| 8 | HTTP 80 | 超文本传输协议 |
| 9 | HTTPS 443 | 超文本传输安全协议 |
| 10 | DHCP 67/68/546 | 动态主机设置协议，c(67), s(68), 546(v6) |
| 11 | | |

DHCP原理图



DHCP服务

本路由器内建的DHCP服务器能自动配置局域网中各计算机的TCP/IP协议。

DHCP服务器:	<input checked="" type="radio"/> 不启用 <input type="radio"/> 启用 选择不启用
地址池开始地址:	192.168.1.100
地址池结束地址:	192.168.1.199
地址租期:	120 分钟 (1~2880分钟, 缺省为120分钟)
网关:	0.0.0.0 (可选)
缺省域名:	
首选DNS服务器:	0.0.0.0 (可选)
备用DNS服务器:	0.0.0.0 (可选)

保存 **帮助**

家用路由器 DHCP设置

1

- 2 DNS称为域名系统，在网站运行中起到了至关重要的作用，主要作用是负责把网站域名解析为对应的IP地址。
- 3 一般域名提供商，提供的dns服务器，都是走udp53端口的。

4

DNS解析过程

域名是什么 ?

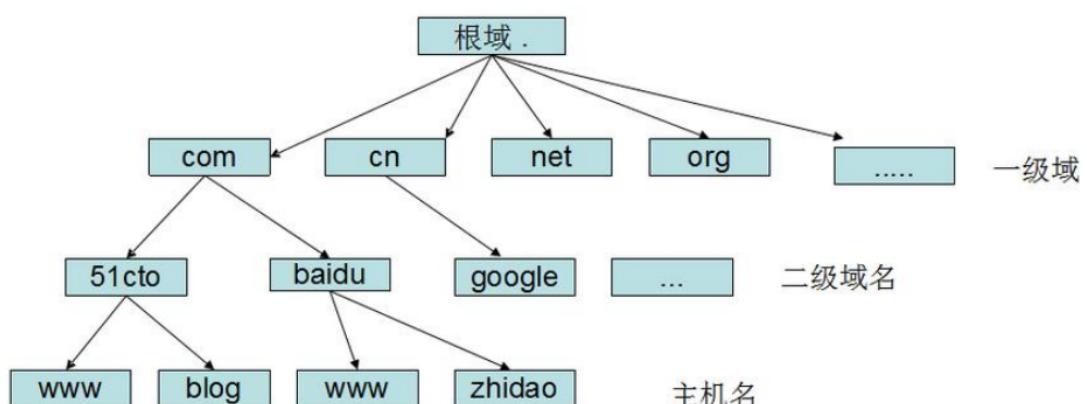
- 1
- 2 举个例子, `https://www.baidu.com`, 这个其实并不是域名, 其中`https`是指协议, 去掉`https`后, `www.baidu.com`. (注意最后面有一个点号) 才是真正的域名。
- 3 `www`对应了一个业务 `www.baidu.com`-->百度的首页
- 4 `news`对应了另一个业务 `news.baidu.com`-->百度的新闻业务
- 5 域名的第二部分: `baidu sina weibo oldboyedu jd taobao` 权威域名。全球唯一 不能冲突
- 6 域名的第三部分: `.com .cn .org .net .中国 .我爱你`
- 7
- 8
- 9
- 10 每个域名的最后面都有一个点号 `"."` 表示根域名, 为了方便在实际使用的时候被省略了。
- 11
- 12 根域名的下一级就是顶级域名了, `.com` 也就是顶级域名, 常见的顶级域名后缀有`.com`、`.cn`、`.net`、`.org` 等, 这些都是固定的, 用户不能自己修改, 只能选择。
- 13
- 14 顶级域名的下一级又是权威域名, 如`baidu.com`中的`.baidu`, 这个权威域名就是我们自己可注册的域名。
- 15 `www.baidu.com www.weibo.com www.linuxnc.com`
- 16 顶级域名下就是主机名了, `www`是指主机名, 这个是我们可以自己定义的, 通常在`http`服务器如`nginx`中可以修改。
- 17
- 18 `http https 协议`
- 19 `.com .cn .org .net. ...` 顶级域名
- 20 `baidu sina weibo linuxnc` 权威域名

21 www.baidu.com --->显示百度的主页
22 news.baidu.com--->显示的百度的新闻页面
23
24 www.baidu.com的www news.baidu.com 的news 表示主机名 表示不同的业务 不同的页面
25
26 .com.
27 .cn.
28 .org.
29
30 .是根域名

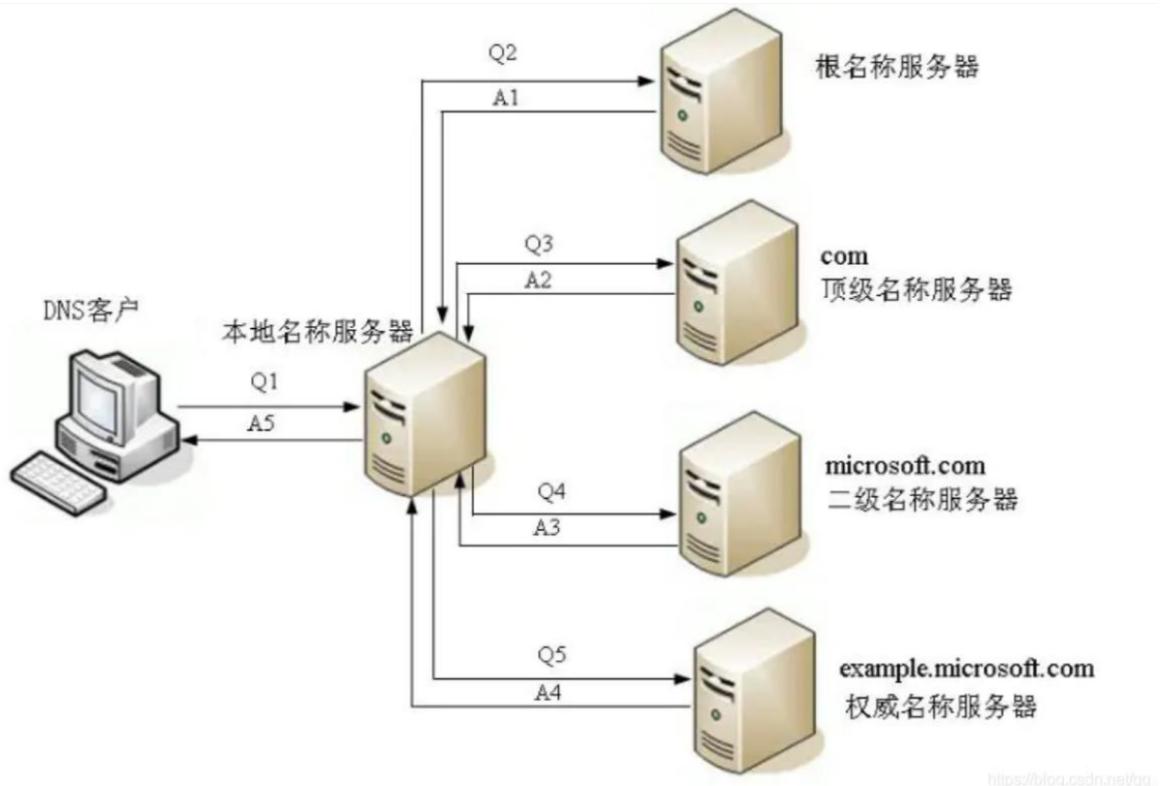
域名解析过程分析

- 1 下面就还以www.baidu.com这个网址来分析一下dns的解析过程。
- 2
- 3 当浏览器拿到输入的www.baidu.com后，首先会去浏览器的dns缓存中去查询是否有对应记录，如果查询到记录就可以直接返回ip地址，完成解析。
- 4
- 5 如果浏览器没有缓存，那就再去查询操作系统的缓存，同样的，如果查询到记录就可以直接返回ip地址，完成解析。
- 6
- 7 如果操作系统也没有缓存，那就再去查看本地hosts文件，windows下host文件一般位于 "C:\Windows\System32\drivers\etc"。
- 8
- 9 近几年网上流传的通过修改本地host文件来避免双11女友剁手的段子，其实就是将淘宝的支付接口解析到错误的ip地址，从而导致支付不成功。
- 10

- 11 如果本地**host**文件也没有相应记录，那就需要求助于本地**dns**服务器了，所以应该要知道本地**dns**的**ip**地址。
- 12 Linux本地**DNS**: 223.5.5.5 LocalDNS LDNS
- 13
- 14 本地**dns**服务器**ip**地址一般是由本地网络服务商如移动、电信提供，一般是通过**DHCP**自动分配，当然你也可以自己手动配置。目前用的比较多的是谷歌提供的公用**dns** 8.8.8.8和国内的公用**dns** 114.114.114.114及阿里的223.5.5.5。
- 15
- 16 你之前可能有遇到过电脑可以正常上**QQ**但是就是不能打开网页的怪现象，这种情况大多数可能就是**dns**域名解析出问题了，你可以尝试手动把**dns**设置为公用**dns**。
- 17
- 18 找到本地**dns**后，它也会先去查询一遍它自己的缓存，如果有记录就返回，如果没有记录，它将开始要去我们前面提到的根域名服务器查询了。注意由于根域名服务器**ip**地址一般都是固定的，所以本地**dns**服务器一般都内置了根域名服务器**ip**地址。<https://www.uedbox.com/post/50977/>
- 19
- 20 目前全球一共有13个根域名服务器（这里并不是指13台服务器，是指13个**ip**地址，按字母a-m编号），为了能更高效完成全球所有域名的解析请求，根域名服务器本身并不会直接去解析域名，而是会把不同的解析请求分配给下面的其他服务器去完成，下面是**dns**域名系统的树状结构图。



- 1 注意dns域名服务器一般分三种，分别是根域名服务器(.)、顶级域名服务器(.com)、权威域名服务(.baidu.com)。
- 2
- 3 当根域名接收到本地dns的解析请求后，发现是后缀是.com，于是就把负责.com的顶级域名服务器ip地址返给本地dns。
- 4
- 5 本地dns拿着返回的ip地址再去找到对应的顶级域名服务器，顶级域名又把负责该域名的权威服务器ip返回去。
- 6
- 7 本地dns又拿着ip去找对应的权威服务器，权威服务器最终把对应的主机ip的解析记录（俗称A记录）返回给本地dns。
- 8
- 9 本地dns会将解析后的ip地址信息进行缓存，缓存好将A记录信息返回给客户端。
- 10
- 11 客户端收到本地dns响应的A记录信息，会将A记录缓存到本地，然后使用解析后的ip地址访问www.baidu.com。
- 12
- 13 至此就完成了域名解析的全过程。
- 14
- 15 下面用一张图来展示上面迭代查询的过程。
- 16



https://blog.csdn.net/qq_

- 1 解析期间涉及到两个特殊查询：
- 2 客户端---本地dns服务器：递归查询
- 3 本地dns服务器---根域名服务器 顶级域名服务器 权威域名服务器：迭代查询
- 4 所谓递归查询过程就是“查询的递交者”更替，而迭代查询过程则是“查询的递交者”不变。
- 5
- 6 A记录：
- 7 从域名到IP的解析过程，被称为A记录；www.baidu.com-->1.1.1.1
- 8
- 9 获取A记录命令方法: `yum -y install bind-utils`
- 10
- 11 1) `dig www.baidu.com`
- 12 `dig @223.5.5.5 www.baidu.com +trace` --显示完整DNS解析过程
- 13 2) `nslookup www.baidu.com`
- 14 3) `host www.baidu.com`
- 15 4) `ping www.baidu.com`
- 16

17 面试题：

18 1. 浏览器输入www.baidu.com 查询浏览器缓存 有返回IP
没有则查询本地的HOSTS

19 2. 如果HOSTS有返回IP 如果没有继续查询本地的DNS

20 3. 本地DNS一般是我们自己配置的比如223.5.5.5 8.8.8
114.114.114.114, 查询本地DNS是否有对应的IP 如果有
返回给浏览器 如果没有则查询.根服务器

21 -----1-3过程称为递归查询-----

22 4. 根服务器不存储域名解析, 会给LDNS返回顶级域.com的
服务器IP地址

23 5. LDNS重新请求.com域名服务器 .com不存在域名解析
.com会返回权威域名服务器的IP地址给LDNS

24 6. LDNS重新请求baidu.com权威域名服务器, 权威域名服务
器就是我们自己配置的A记录解析, 将A记录对应的IP地址返
回给LDNS

25 7. LDNS拿到后自己缓存一份 返回给浏览器一份

26 8. 浏览器和拿到的百度服务器IP地址建立连接

27 -----迭代查询 有去有回

28

29 1. 浏览器--->本地HOSTS-->LDNS--->

30 2. LDNS--->根 根返回 顶级域.com

31 3. LDNS--->顶级域 顶级域返回权威域

32 4. LDNS--->权威域服务器 权威域名返回 A记录解析对应
的服务器IP地址

33 5. 浏览器-->百度IP建立连接

34

4. 主机到主机层协议介绍

1 TCP：传输控制协议, 是一种面向连接的、可靠的、基于字节
流的传输层通信协议。

2

3 特点：面向连接，可靠，传输效率低

4
5 应用场景: **web**浏览器, 电子邮件, 文件传输程序
6
7 外卖员-->快递必须送到我们的手中
8
9 **UDP**: 用户数据报协议, 属于无连接的传输协议
10
11 特点: 无连接、不可靠、快速传输
12
13 应用场景: 域名系统 (**DNS**), 视频流, **IP**语音
 (**VOIP**)
14 外卖员-->快递放在门口
15
16
17 **TCP UDP**协议端口号范围 1 - 65535 (可以的), 真正
 端口号总数为2的16次方=**65536**
18
19 面向连接: 是指通信双方在通信时, 要事先建立一条通信线
 路, 其有三个过程: 建立连接、使用连接和释放连接。
20
21 面向无连接: 是指通信双方不需要事先建立一条通信线路,
 而是把每个带有目的地址的包 (报文分组) 送到线路上, 由
 系统自主选定路线进行传输。

5. 控制字段介绍

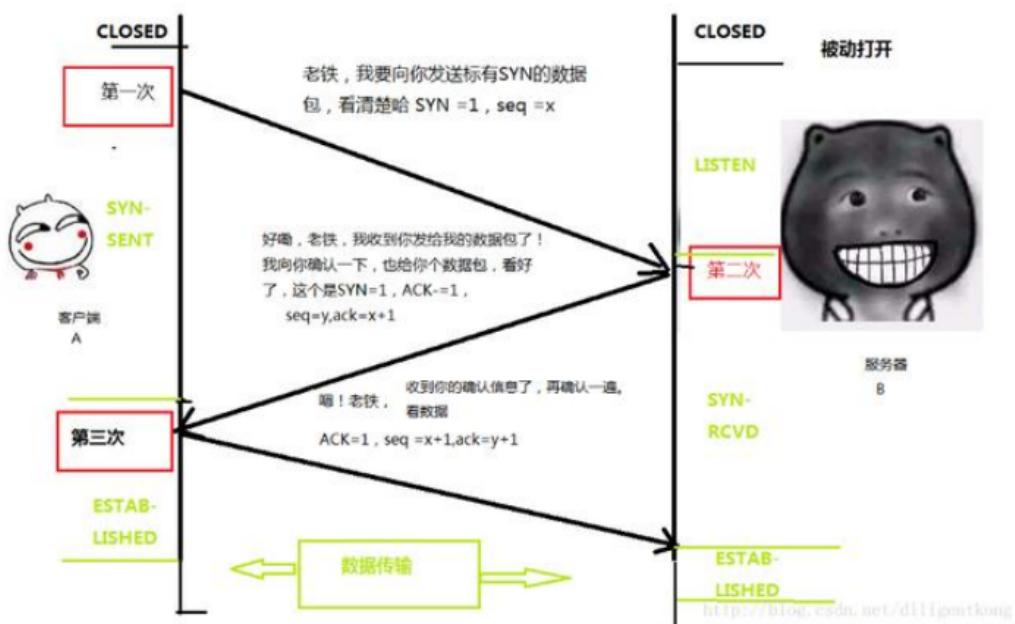
- 1 **ACK:** 表示确认控制字段，确认数据是否接收到
- 2 **SYN:** 表示请求建立连接字段，和主机建立连接时使用
- 3 **FIN:** 表示请求断开连接字段，和主机断开连接时使用
- 4 **PSH:** 表示有**DATA**数据传输，**PSH**为**1**表示的是有真正的**TCP**数据包内容被传递
- 5 **RST:** 表示连接重置。一般是在**FIN**之后才会出现为**1**的情况，表示的是连接重置。
- 6 **seq**序列号：将大的数据进行拆分后标记序列信息，便于接收方将拆分后的数据信息进行组装，在原有序列号基础上**+1**进行回复，告知发送方下次再给我发送的数据是什么

7

注意：传输数据包，没有真正数据信息（三次握手过程），传输数据过程，在三次握手之后。

6. TCP三次握手

TCP三次握手过程如下图所示：



- 1 服务端：
2 **CLOSED**--->启动服务**LISTEN**监听
- 3 客户端：
4 **CLOSED**--->发送第一个请求后 **SYN_SENT**
- 5
- 6 服务端：
7 **LISTEN**--->第一次响应客户端后 **SYN_RCVD** 同步已发送状态
- 8
- 9 客户端：
10 **SYN_SENT**-->发送第三次数据包后 **ESTABLISHED**建立连接状态
- 11
- 12 服务端：
13 **SYN_RCVD**-->收到客户端第三次数据后**ESTABLISHED** 建立连接
- 14
- 15
- 16 **TCP**是面向连接的，无论哪一方向另一方发送数据之前，都必须先在双方之间建立一条连接。
- 17
- 18 刚开始，客户端和服务器都处于**CLOSED**状态。
- 19
- 20 此时，客户端向服务器主动发出连接请求，服务器被动接受连接请求。
- 21
- 22 1. **TCP**服务器进程先创建传输控制块**TCB**，时刻准备接受客户端进程的连接请求，此时服务器就进入了**LISTEN**（监听）状态。
- 23

24 2. TCP客户端进程也是先创建传输控制块**TCB**，然后向服务器发出连接请求报文，此时报文首部中的同步标志位**SYN=1**，同时选择一个初始序列号**seq = x**，此时TCP客户端进程进入了**SYN-SENT**（同步已发送状态）状态。TCP规定，SYN报文段（**SYN=1**的报文段）不能携带数据，但需要消耗掉一个序号。

25

26 3. TCP服务器收到请求报文后，如果同意连接，则发出确认报文。确认报文中的**ACK=1**，**SYN=1**，确认序号是**x + 1**，同时也要为自己初始化一个序列号**seq = y**，此时TCP服务器进程进入了**SYN-RCVD**（同步收到）状态。这个报文也不能携带数据，但是同样要消耗一个序号。

27

28 4. TCP客户端进程收到确认后还要向服务器给出确认。确认报文的**ACK=1**，确认序号是**y + 1**，自己的序列号是**x + 1**。

29

30 5. 此时TCP连接建立，客户端进入**ESTABLISHED**（已建立连接）状态。当服务器收到客户端的确认后也进入**ESTABLISHED**状态，此后双方就可以开始通信了。

31

32 举个栗子：

33

34 TCP三次握手好比在一个夜高风黑的夜晚，你一个人在小区里散步，不远处看见小区里的一位漂亮妹子迎面而来，但是因为路灯有点暗等原因不能100%确认，所以要通过招手的方式来确定对方是否认识自己。

35

36 你首先向妹子招手(**syn**)，妹子看到你向自己招手后，向你点了点头挤出了一个微笑(**ack**)。同时妹子也向你招了招手(**syn**)，你看到妹子向自己招手后知道对方是在寻求自己的确认，于是也点了点头挤出了微笑(**ack**)。

37

38 于是两人加快步伐，走到了一起。

39

40 我们来回顾一下，这个过程中总共有四个动作，

41

42 你招手

43 妹子点头微笑

44 妹子招手

45 你点头微笑

46

47 其中妹子连续进行了两个动作，先是点头微笑(回复对方)，然后再次招手(寻求确认)，实际上我们可以将这两个动作合成一个动作，招手的同时点头和微笑(**syn+ack**)。于是这四个动作就简化成了三个动作。

48

49 你招手

50 妹子点头微笑并招手

51 你点头微笑

52

53 这就是三次握手的本质，中间的一次动作是两个动作的合并。通过这个案例，不知你对**TCP**三次握手，有没有进一步的理解。

54

55

56 三次握手面试题：

57 1. 伟苹想和仓姐姐搞对象，我想和你搞对象**SYN=1**，并且送给仓姐姐第一个礼物**seq=x**

58 2. 仓姐姐说收到了你的渴望**ACK=1**。我也想和你搞对象**SYN=1**，并且也给伟苹送了第一个礼物**seq=y**。并且和你说你下次应该给我第二个礼物了**Ack=x+1**

59 3. 伟苹确认收到了苍姐姐的信息**ACK=1**。并且给苍姐姐第二个礼物**seq=x+1**，并且说苍姐姐你下次应该给我第二个礼物了**Ack=y+1**。

60 4. 伟苹和仓姐姐连接成功。

61

62

63 1.A向B请求建立连接 SYN=1 seq=x

64 2.B向A回复 ACK=1 SYN=1 seq=y ,Ack=x+1

65 3.A向B回复 ACK=1,seq=x+1,Ack=y+1

66

67

68 重点：

69 OSI七层模型

70 TCP/IP四层模型

71 DNS解析

72 TCP三次握手

73 TCP和UDP区别

74

为什么要三次握手

1 为了防止已失效的连接请求报文段突然又传到了服务端，因而产生错误。

2

3 举个栗子：

4

5 “已失效的连接请求报文段”的产生在这样一种情况下：客户端发出的第一个连接请求报文段并没有丢失，而是在某个网络结点长时间的滞留了，以致延误到连接释放以后的某个时间才到达服务端。本来这是一个早已失效的报文段。但服务端收到此失效的连接请求报文段后，就误认为是客户端再次发出一个新的连接请求。于是就向客户端发出确认报文段，同意建立连接。假设不采用“三次握手”，那么只要服务端发出确认，新的连接就建立了。由于现在客户端并没有发出建立连接的请求，因此不会理睬服务端的确认，也不会向服务端发送数据。但服务端却以为新的运输连接已经建立，并一直等待客户端发来数据。这样，服务端的很多资源就白白浪费掉了。采用“三次握手”的办法可以防止上述现象发生。例如刚才那种情况，客户端不会向服务端的确认发出确认。服务端由于收不到确认，就知道客户端并没有要求建立连接。”

6

7 这就很明白了，防止了服务器端的一直等待而浪费资源。

7. TCP四次挥手

1 数据传输完毕后，双方都可以释放连接。

2

3 此时客户端和服务器都是处于**ESTABLISHED**状态，然后客户端主动断开连接，服务器被动断开连接。

4

5 1. 客户端进程发出连接释放报文，并且停止发送数据。

6 释放数据报文首部, $FIN=1$, 其序列号为 $seq = u$ (等于前面已经传送过来的数据的最后一个字节的序号加1), 此时客户端进入 **FIN-WAIT-1** (终止等待1) 状态。TCP规定, **FIN**报文段即使不携带数据, 也要消耗一个序号。

7

8 2. 服务器收到连接释放报文, 发出确认报文, $ACK=1$, 确认序号为 $u + 1$, 并且带上自己的序列号 $seq = v$, 此时服务端就进入了 **CLOSE-WAIT** (关闭等待) 状态。

9 TCP服务器通知高层的应用进程, 客户端向服务器请求了断开连接, 这时候处于半关闭状态, 即客户端已经没有数据要发送了, 但是服务器若发送数据, 客户端依然要接受。这个状态还要持续一段时间, 也就是整个 **CLOSE-WAIT** 状态持续的时间。

10

11 3. 客户端收到服务器的确认请求后, 此时客户端就进入 **FIN-WAIT-2** (终止等待2) 状态, 等待服务器发送连接释放报文 (在这之前还需要接受服务器发送的最终数据)

12

13 4. 服务器将最后的数据发送完毕后, 就向客户端发送连接释放报文, $FIN=1$, 确认序号为 $v + 1$, 由于在半关闭状态, 服务器很可能又发送了一些数据, 假定此时的序列号为 $seq = w$, 此时服务器就进入了 **LAST-ACK** (最后确认) 状态, 等待客户端的确认。

14

15 5. 客户端收到服务器的连接释放报文后, 必须发出确认, $ACK=1$, 确认序号为 $w + 1$, 而自己的序列号是 $u + 1$, 此时客户端就进入了 **TIME-WAIT** (时间等待) 状态。注意此时TCP连接还没有释放, 必须经过 $2*MSL$ (最长报文段寿命) 的时间后, 当客户端撤销相应的TCB后, 才进入 **CLOSED** 状态。

16

17 6. 服务器只要收到了客户端发出的确认，立即进入**CLOSED**状态。同样，撤销**TCB**后，就结束了这次的**TCP**连接。可以看到，服务器结束**TCP**连接的时间要比客户端早一些。

18

19 小知识点：在网络传输层，**tcp**模块中有一个**tcb**（传输控制模块，**transmitcontrolblock**），它用于记录**tcp**协议运行过程中的变量。对于有多个连接的**tcp**，每个连接都有一个**tcb**。**tcb**结构的定义包括这个连接使用的源端口、目的端口、目的**ip**、序号、应答序号、对方窗口大小、己方窗口大小、**tcp**状态、**top**输入/输出队列、应用层输出队列、**tcp**的重传有关变量。

20

21

22

23 四次挥手：

24 1. 伟萍向苍姐姐发送分手的请求。我要和你分手 FIN

25 2. 苍姐姐收到回复 好的收到了 ACK

26 3. 苍姐姐发送给伟萍 我们分手吧 FIN

27 4. 伟萍回复 好的分吧 ACK

28

29 SYN 请求建立连接

30 ACK 确认收到

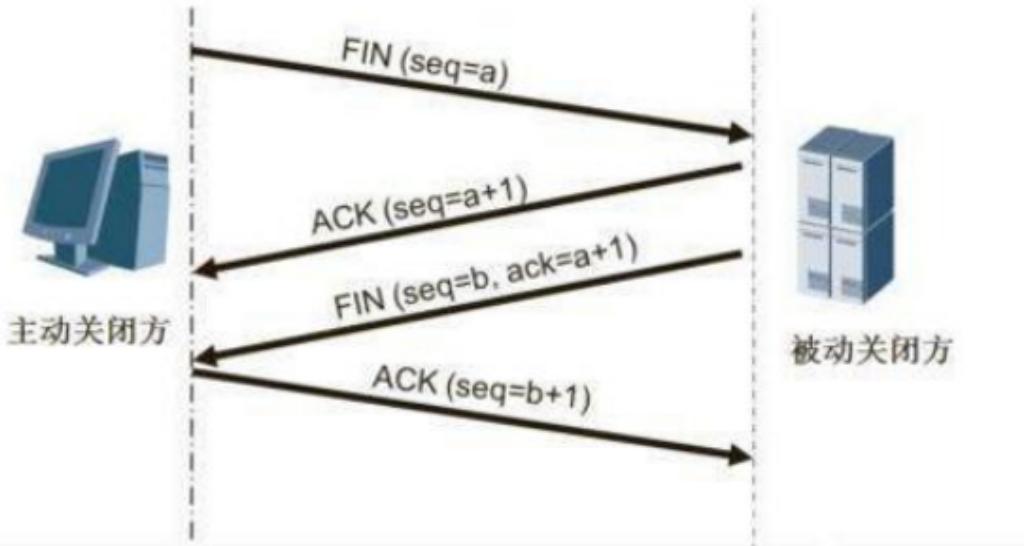
31 seq 序列号

32 Ack 确认下次的序列号

33 FIN 分开 断开连接

34

35



为什么要四次分手？

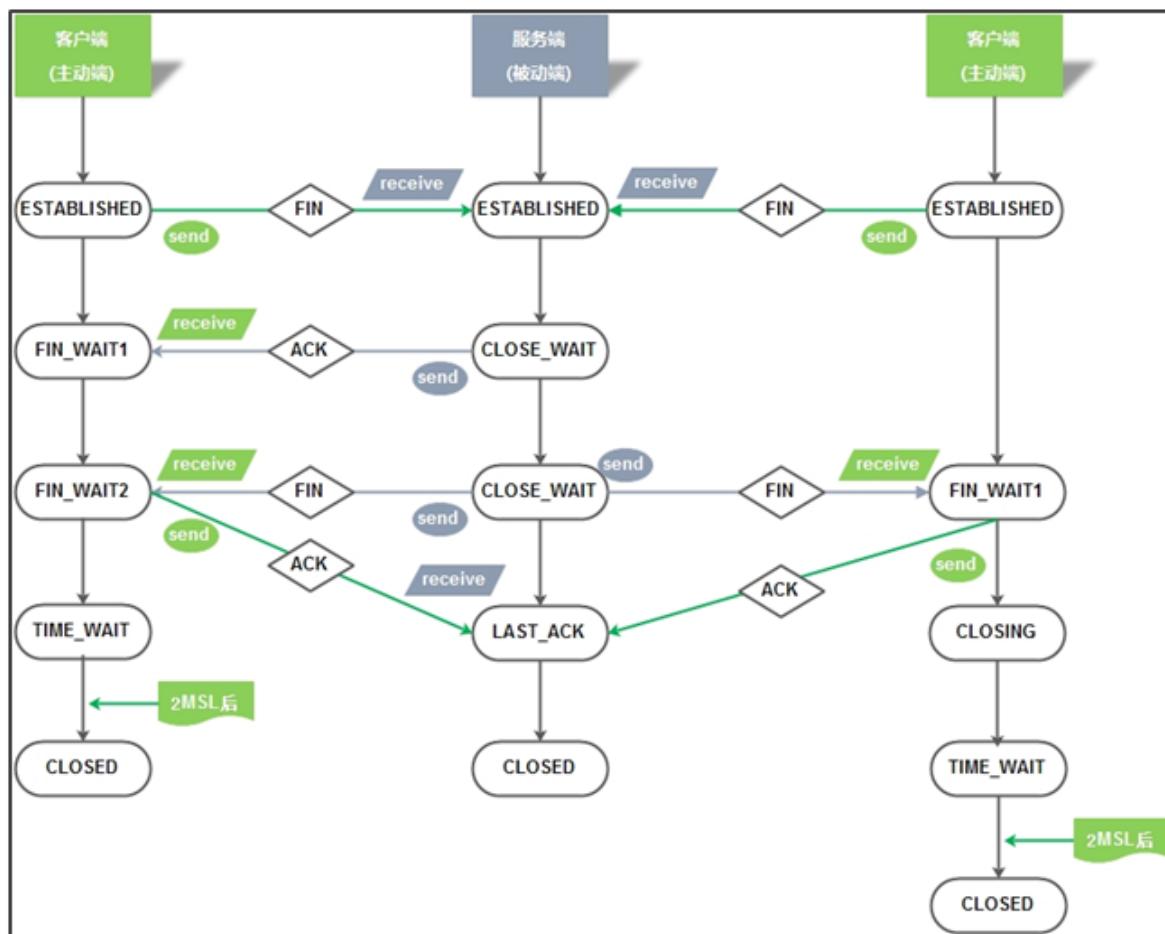
1 那四次分手又是为何呢？TCP协议是一种面向连接的、可靠的、基于字节流的传输层通信协议。TCP是全双工模式，这就意味着，当主机1发出FIN报文段时，只是表示主机1已经没有数据要发送了，主机1告诉主机2，它的数据已经全部发送完毕了；但是，这个时候主机1还是可以接受来自主机2的数据；当主机2返回ACK报文段时，表示它已经知道主机1没有数据发送了，但是主机2还是可以发送数据到主机1的；当主机2也发送了FIN报文段时，这个时候就表示主机2也没有数据要发送了，就会告诉主机1，我也没有数据要发送了，主机1收到主机2的FIN报文段时，回复ACK，表示知道主机2也没有数据传输了，之后彼此就会愉快的中断这次TCP连接。

为什么TIME_WAIT 状态还需要等2*MSL秒之后才能返回到CLOSED 状态呢？

1 因为虽然双方都同意关闭连接了，而且握手的4个报文也都发送完毕，按理可以直接回到CLOSED状态（就好比从SYN_SENT状态到ESTABLISH状态那样），但是我们必须假想网络是不可靠的，你无法保证你最后发送的ACK报文一定会被对方收到，就是说对方处于LAST_ACK状态下的SOCKET可能会因为超时未收到ACK报文，而重发FIN报文，所以这个TIME_WAIT状态的作用就是用来重发可能丢失的ACK报文。

2

8. TCP协议的十一种状态集转换



TCP11种状态集表示含义

- 1 客户端发送FIN给服务端-->ESTABLISHED-->FIN_WAIT1
第一次等待
- 2 服务端收到回复ACK：ESTABLISHED--->CLOSE_WAIT
关闭等待
- 3 收到后客户端：FIN_WAIT1-->FIN_WAIT2第二次等待

4 服务端继续回复客户端**FIN: CLISED_WAIT---**
>**LAST_ACK**

5 客户端回复确认**ACK: FIN_WAIT2-->TIME_WAIT**时间等待-->**CLOSED**状态

6 最后服务端收到确认**ACK: LAST_ACK--> CLOSED**

7

8

9 各个状态的意义如下:

10

11 **CLOSED**: 初始状态, 表示**TCP**连接是“关闭着的”或“未打开的”。

12

13 **LISTEN** : 表示服务器端的某个**SOCKET**处于监听状态, 可以接受客户端的连接。

14

15 **SYN_RCVD** : 表示服务器接收到了来自客户端请求连接的**SYN**报文。在正常情况下, 这个状态是服务器端的**SOCKET**在建立**TCP**连接时的三次握手会话过程中的一个中间状态, 很短暂, 基本上用**netstat**很难看到这种状态, 除非故意写一个监测程序, 将三次**TCP**握手过程中最后一个**ACK**报文不予发送。当**TCP**连接处于此状态时, 再收到客户端的**ACK**报文, 它就会进入到**ESTABLISHED**状态。

16

17 **SYN_SENT** : 这个状态与**SYN_RCVD**状态相呼应, 当客户端**SOCKET**执行**connect()**进行连接时, 它首先发送**SYN**报文, 然后随即进入到**SYN_SENT**状态, 并等待服务端的发送三次握手中的第2个报文。**SYN_SENT**状态表示客户端已发送**SYN**报文。

18

19 **ESTABLISHED** : 表示**TCP**连接已经成功建立。

20

- 21 **FIN_WAIT_1** : 这个状态得好好解释一下, 其实**FIN_WAIT_1**和**FIN_WAIT_2**两种状态的真正含义都是表示等待对方的**FIN**报文。而这两种状态的区别是:
FIN_WAIT_1状态实际上是当**SOCKET**在**ESTABLISHED**状态时, 它想主动关闭连接, 向对方发送了**FIN**报文, 此时该**SOCKET**进入到**FIN_WAIT_1**状态。而当对方回应**ACK**报文后, 则进入到**FIN_WAIT_2**状态。当然在实际的正常情况下, 无论对方处于任何种情况下, 都应该马上回应**ACK**报文, 所以**FIN_WAIT_1**状态一般是比较难见到的, 而**FIN_WAIT_2**状态有时仍可以用**netstat**看到。
- 22
- 23 **FIN_WAIT_2** : 上面已经解释了这种状态的由来, 实际上**FIN_WAIT_2**状态下的**SOCKET**表示半连接, 即有一方调用**close()**主动要求关闭连接。注意: **FIN_WAIT_2**是没有超时的(不像**TIME_WAIT**状态), 这种状态下如果对方不关闭(不配合完成4次挥手过程), 那这个**FIN_WAIT_2**状态将一直保持到系统重启, 越来越多的**FIN_WAIT_2**状态会导致内核崩溃。
- 24
- 25 **TIME_WAIT** : 表示收到了对方的**FIN**报文, 并发送出了**ACK**报文。**TIME_WAIT**状态下的**TCP**连接会等待 $2 * MSL$ (**Max Segment Lifetime**, 最大分段生存期, 指一个**TCP**报文在**Internet**上的最长生存时间。每个具体的**TCP**协议实现都必须选择一个确定的**MSL**值, **RFC 1122**建议是2分钟, 但**BSD**传统实现采用了30秒, **Linux**可以**cat /proc/sys/net/ipv4/tcp_fin_timeout**看到本机的这个值), 然后即可回到**CLOSED**可用状态了。如果**FIN_WAIT_1**状态下, 收到了对方同时带**FIN**标志和**ACK**标志的报文时, 可以直接进入到**TIME_WAIT**状态, 而无须经过**FIN_WAIT_2**状态。(这种情况应该就是四次挥手变成三次挥手的那种情况)
- 26

27 **CLOSING** : 这种状态在实际情况中应该很少见，属于一种比较罕见的例外状态。正常情况下，当一方发送**FIN**报文后，按理来说是应该先收到（或同时收到）对方的**ACK**报文，再收到对方的**FIN**报文。但是**CLOSING**状态表示一方发送**FIN**报文后，并没有收到对方的**ACK**报文，反而却也收到了对方的**FIN**报文。什么情况下会出现此种情况呢？那就是当双方几乎在同时**close()**一个**SOCKET**的话，就出现了双方同时发送**FIN**报文的情况，这是就会出现**CLOSING**状态，表示双方都正在关闭**SOCKET**连接。

28

29 **CLOSE_WAIT** : 表示正在等待关闭。怎么理解呢？当对方**close()**一个**SOCKET**后发送**FIN**报文给自己，你的系统毫无疑问地将会回应一个**ACK**报文给对方，此时**TCP**连接则进入到**CLOSE_WAIT**状态。接下来呢，你需要检查自己是否还有数据要发送给对方，如果没有的话，那你也就可以**close()**这个**SOCKET**并发送**FIN**报文给对方，即关闭自己到对方这个方向的连接。有数据的话则看程序的策略，继续发送或丢弃。简单地说，当你处于**CLOSE_WAIT**状态下，需要完成的事情是等待你去关闭连接。

30

31 **LAST_ACK** : 当被动关闭的一方在发送**FIN**报文后，等待对方的**ACK**报文的时候，就处于**LAST_ACK**状态。当收到对方的**ACK**报文后，也就可以进入到**CLOSED**可用状态了。

32

33

34

35 重点小结：

36 1. OSI七层模型

37 应用层 表示层 会话层 传输层 网络层 数据链路层 物理层

38 2. DNS解析流程

39 3. TCP三次握手

40 4. TCP四次挥手

9. 因特网层协议介绍

- 1 ICMP Internet控制报文协议。它是TCP/IP协议簇的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。
- 2
- 3 RARP 反向地址转换协议
- 4
- 5 ARP 地址解析协议，是根据IP地址获取物理地址的一个TCP/IP协议。作用：有效的避免广播风暴的产生
- 6
- 7 动态ARP：自动完善ARP表信息，会定时更新ARP条目，自动更新ARP表时会消耗服务器性能，适用于主机更换频繁网络。
- 8 静态ARP：手工配置ARP表信息，不会实时更新ARP条目，节省服务器性能，适用于主机更换不频繁网络。

10. 网络接入层介绍

- 1 **Ethernet** 以太网（Ethernet）是一种计算机局域网技术。
- 2
- 3 **FastEth** 快速以太网（Fast Ethernet）是一类新型的局域网，其名称中的“快速”是指数据速率可以达到 **100Mbps**，是标准以太网的数据速率的十倍。
- 4
- 5 **Token Ring** 令牌环网（Token Ring）是一种LAN协议，其中所有的工作站都连接到一个环上，每个工作站只能同直接相邻的工作站传输数据。
- 6
- 7 **FDDI** 光纤分布式数据接口，在光缆网络上发送数字和音频信号的一组协议。

6. IP地址

1. IP地址基本概念

- 1 **IP地址**（Internet Protocol Address）是指互联网协议地址，又译为网际协议地址。
- 2
- 3 **IP地址**在网络层将不同的物理网络地址统一到了全球唯一的**IP地址**上（屏蔽物理网络差异），是唯一标识互联网上计算机的逻辑地址（相当于手机号码，可以通过唯一的手机号码找到手机），所以**IP地址**也被称为互联网地址（可见其重要性）。

2. IP地址格式

1 我们目前常用的**IPv4**中规定，**IP**地址长度为32位二进制，在表示时，一般将32位地址拆分为4个8位二进制，再转为4个十进制数表示，每个数字之间用点隔开，如
2 **127.0.0.1** (**localhost**)，这种描述方式被称为“点-数表示法”点分十进制。

3

4 **11111111 11111111 11111111 11111111**

5

6 0 0 0 0 0 0 0 1 二进制

7 0 0 0 0 0 0 1 1 十进制

8 0 0 0 0 0 1 0

9 0 0 0 0 0 1 2 十进制

10 0 0 0 0 0 1 1

11 0 0 0 0 1 0 3 十进制

12

13 1 1 1 1 1 1 1 1

14 128 64 32 16 8 4 2 1

15

16

17 二进制转十进制算法：将每个为1的位置相加得到十进制

18 0 0 0 0 0 1 0 1 转换成十进制 等于 5

19 0 1 0 0 0 0 0 0 转换成十进制 等于 64

20 1 1 0 0 0 0 0 0 转换成十进制 等于 192

21 1 1 1 1 1 1 1 1 转出成十进制 等于 255

22

23

24

25

26

27

28 十进制转二进制：对每位为1的相减 做减法运算

```

29 1   1   1   1   1   1   1   1
30 128 64  32  16   8   4   2   1
31 68十进制转换成二进制
32 68-64=4
33 4-4=0
34 0   1   0 0  0   1   0   0
35
36 172十进制转换成二进制
37 172-128=44
38 44-32=12
39 12-8=4
40 4-4=0
41 1   0   1   0   1   1 0 0
42
43
44 192.168.13.253
45 192   =   1 1 0 0 0 0 0 0 0
46 168   =   1 0 1   0 1   0 0 0
47 13    =   0 0 0 0 1 1 0 1
48 253   =   1 1 1 1 1 1 0 1
49
50
51
52
53
54
55 IP地址层次：分为网络号和主机号两个层次。网络号表示主机所属网络，主机号表示主机本身。网络号与主机号的位数与IP地址分类有关。

```

192.	168.	10.	1
11000000	10101000	00001010	00000001

IP地址十进制与二进制对应关系

十进制数	二进制数	十进制数	二进制数
1	1	11	1011
2	10	12	1100
3	11	13	1101
4	100	14	1110
5	101	15	1111
6	110	16	10000
7	111	17	10001
8	1000	18	10010
9	1001	19	10011
10	1010	20	10100

十进制数	二进制数	二进制	十进制数	二进制数	二进制
1	1	00001	11	1011	01011
2	10	00010	12	1100	01100
3	11	00011	13	1101	01101
4	100	00100	14	1110	01110
5	101	00101	15	1111	01111
6	110	00110	16	10000	10000
7	111	00111	17	10001	10001
8	1000	01000	18	10010	10010
9	1001	01001	19	10011	10011
10	1010	01010	20	10100	10100

二级制与十进制对应数值表。

根据第两张表的信息进行数据的逻辑总结可以得知如下结论：

二进制	00001	00010	00100	01000	10000
逻辑运算	2的0次方	2的1次方	2的2次方	2的3次方	2的4次方
十进制	1	2	4	8	16

二级制转换十进制公式表。

因此可以得知对于点分十进制而言，对应的每个数值即为下图所示：

二进制	10000000	01000000	00100000	00010000	00001000	00000100	00000010	00000001
逻辑运算	2的7次方	2的6次方	2的5次方	2的4次方	2的3次方	2的2次方	2的1次方	2的0次方
十进制	128	64	32	16	8	4	2	1

二级制转换十进制公式表。

根据上面说到的将 32 位数字分为 4 端，即每段 8 位数字；通过上图也可以得知主机地址的初步理解算法。

192.	168.	10.	1
11000000	10101000	00001010	00000001

IP地址十进制与二进制对应关系。

3. IP地址分配

1 | IP地址分配的基本原则是：要为同一网络（子网、网段）内不同主机分配相同的网络号，不同的主机号。

4. IP地址类型

1 #公有地址

2 公有地址 (Public address) 由 Internet
NIC (Internet Network Information Center 因特
网信息中心) 负责。这些 IP 地址分配给注册并向 Internet NIC
提出申请的组织机构。通过它直接访问因特网。全球唯一，
不能出现重复。

3

4 #私有地址

5 私有地址 (Private address) 属于非注册地址，专
门为组织机构内部使用。缓解了地址枯竭 是可以重复使用的
(不同局域网内)

6

7 #以下列出留用的内部私有地址

8 A类 10.0.0.0--10.255.255.255
9 10.0.0.1-10.0.0.254
10 10.0.1.1=10.0.1.254
11 10.0.2.1=10.0.2.254
12 10.1.0.1=10.1.0.1=10.1.0.254

13

14

15 B类 172.16.0.0--172.31.255.255
16 172.16.0.1-172.16.0.254
17 172.16.1.1-172.16.1.254
18 11111111=255

19 C类 192.168.0.0--192.168.255.255
20 192.168.0.1-192.168.0.254
21 192.168.1.1-192.168.1.254
22 192.168.2.1-192.168.2.254

23

24 需要实现配置私网地址的服务器可以访问外网 (互联
网) ? ? ?

25

5. IP地址常见分类

1 #A类IP地址

2

3 一个A类IP地址是指，在IP地址的四段号码中，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。如果用二进制表示IP地址的话，A类IP地址就由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”。A类IP地址中网络的标识长度为8位，主机标识的长度为24位，A类网络地址数量较少，有126个网络，每个网络可以容纳主机数达1600多万台。

4

5 A类IP地址 地址范围1.0.0.1到127.255.255.254（二进制表示为：00000001 00000000 00000000 00000001 - 01111111 11111111 11111111 11111110）。最后一个地址是广播地址。

6

7 A类IP地址的子网掩码为255.0.0.0，每个网络支持的最大主机数为256的3次方-2=16777212台。

8

9 #B类IP地址

10

11 一个B类IP地址是指，在IP地址的四段号码中，前两段号码为网络号码。如果用二进制表示IP地址的话，B类IP地址就由2字节的网络地址和2字节主机地址组成，网络地址的最高位必须是“10”。B类IP地址中网络的标识长度为16位，主机标识的长度为16位，B类网络地址适用于中等规模的网络，有16384个网络，每个网络所能容纳的计算机数为6万多名。

12

- 13 B类IP地址地址范围128.0.0.1-191.255.255.254 (二进制表示为: 10000000 00000000 00000000 00000001----10111111 11111111 11111111 11111110)。最后一个广播地址。
- 14
- 15 B类IP地址的子网掩码为255.255.0.0, 每个网络支持的最大主机数为256的2次方-2=65534台。
- 16
- 17 #C类IP地址
- 18
- 19 一个C类IP地址是指, 在IP地址的四段号码中, 前三段号码为网络号码, 剩下的一段号码为本地计算机的号码。如果用二进制表示IP地址的话, C类IP地址就由3字节的网络地址和1字节主机地址组成, 网络地址的最高位必须是“110”。C类IP地址中网络的标识长度为24位, 主机标识的长度为8位, C类网络地址数量较多, 有209万余个网络。适用于小规模的局域网络, 每个网络最多只能包含254台计算机。
- 20
- 21 C类IP地址范围192.0.0.1-223.255.255.254 (二进制表示为: 11000000 00000000 00000000 00000001 - 11011111 11111111 11111111 11111110)。
- 22
- 23 C类IP地址的子网掩码为255.255.255.0, 每个网络支持的最大主机数为256-2=254台
- 24
- 25 #D类地址用于多点广播 (Multicast)。
- 26
- 27 D类IP地址在历史上被叫做多播地址(multicast address), 即组播地址。在以太网中, 多播地址命名了一组应该在这个网络中应用接收到一个分组的站点。多播地址的最高位必须是“1110”, 范围从224.0.0.0到239.255.255.255。
- 28

29 #E类IP地址

30

31 以“11110”开始，为将来使用保留。

6. 特殊的IP地址

- 1 1.每一个字节都为0的地址（“0.0.0.0”）对应于当前主机；
- 2
- 3 2. IP地址中的每一个字节都为1的IP地址（“255. 255. 255. 255”）是当前子网的广播地址；
- 4
- 5 3. IP地址中凡是以“11110”开头的E类IP地址都保留用于将来和实验使用。
- 6
- 7 4. IP地址中不能以十进制“127”作为开头，该类地址中数字127. 0. 0. 1到127. 255. 255. 255用于回路测试，如：127.0.0.1可以代表本机IP地址，用“<http://127.0.0.1>”就可以测试本机中配置的web服务器。
- 8
- 9 5. 169.254.0.0~169.254.255.255，是开启了dhcp服务的设备但又无法获取到dhcp的会随机使用这个网段的ip
- 10
- 11 总结：3类
- 12 A类 前1位网络位置 后三位主机位
13 127.0.0.1 127.255.255.254
- 14 B类：前2位网络位置 后2位主机位
15 130.0.0.1 130.0.255.254
- 16 C类：前3位网络位置 后1位为主机位
17 192.168.13.1 192.168.13.254
- 18

7. 子网掩码

1 子网掩码又叫网络掩码、地址掩码

2

3 上面我们说到IP地址分为网络号与主机号，但是路由如何区分网络号与主机号呢？就需要通过子网掩码。子网掩码必须与IP地址结合使用，A、B、C类的子网掩码分别为255.0.0.0，255.255.0.0与255.255.255.0（网络号字节为255，主机号字节为0）。

4

5 也就是说给你一个IP地址，那么怎么知道它的网络号和主机号各是多少位呢？

6

7 如果不指定，就不知道哪些位是网络号、哪些是主机号，这就需要通过子网掩码来实现

8

9 子网掩码的重要作用：就是将某个IP地址划分成网络地址和主机地址两部分。

10

11 子网掩码的位数就是网络的位数。A类网络的网络位数是8位，子网掩码就是255.0.0.0，B类网络的网络位数是16位，子网掩码是255.255.0.0，C类是24位，255.255.255.0。

12

13 /8 255.0.0.0

14 /16 255.255.0.0

15 /24 255.255.255.0

16

1. 例1：不同子网下的主机能否直接通信（是否在同一网络/段下）

- 1 假设两个IP地址分别是172.20.0.18和172.20.1.16，子网掩码都是255.255.255.0。
- 2
- 3 我们可以知道两者的网络标识分别是172.20.0和172.20.1，无法直接通信，也就无法PING通。要想能相互通信，需要将子网掩码改成255.255.0.0

2. 如何理解172.20.1.0/18

11111111 11111111 11000000 00000000

255.255.192.0

为什么要子网划分

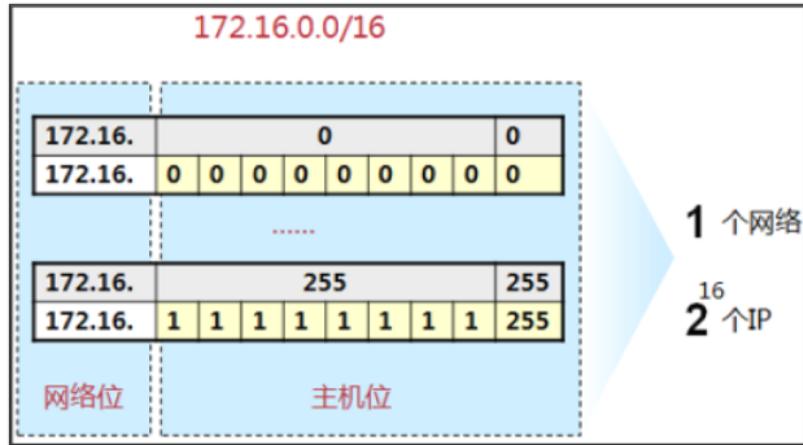
- 1 一个大的地址范围区域，你不进行划分的时候，会造成地址浪费
- 2 一个大的地址范围区域，可能会产生大量广播风暴，影响主机性能
- 3 一个大的地址访问区域，可能会造成网关路由器负载过高
- 4
- 5 将一个大的网段切割成一个一个小的局域网段，就称为子网划分
- 6
- 7 一个网段中可以有多少个地址=2的n次方-2 n表示的就是这个网段中有多少个主机位
- 8 -2 表示网络地址不能用 表示广播地址不能用
- 9 一个局域网中的地址在使用时要预留一个作为网关地址
- 10

掩码地址的表示方式

	网络位				主机位	
IP地址	192	168	1	10		
对应掩码	255	255	255	0		
十进制	11111111	11111111	11111111	00000000	/24	

掩码地址表示

根据掩码如何进行子网划分



B类地址主机位地址范围表示

网络位向右移动，占用主机位，即向主机位借位，生成新的网络位

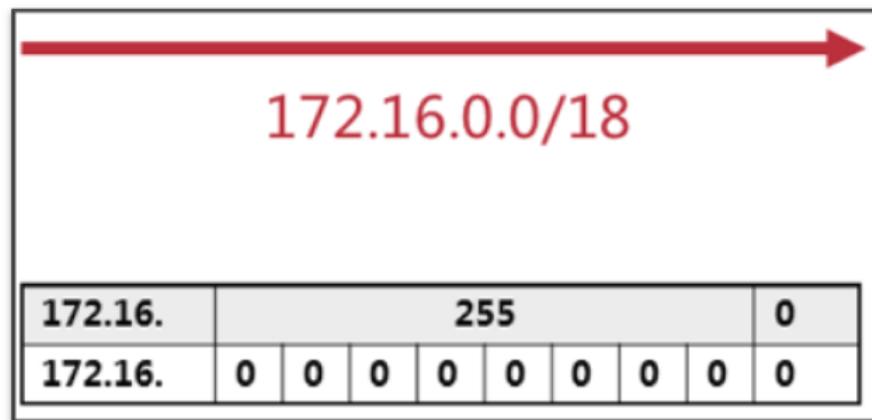
其中/16就表示了子网掩码所指定的网络位个数，A类一般是/8 B类一般是/16 C类/24



B类地址子网化主机位地址范围表示

实质上就是移动网络位和主机位中间分隔的线，向主机位进行移动，减少主机数量，扩大拥有的子网数量；新的子网产生，掩码表示的信息也要进行变化，从而可以更好的表示网络地址的规划情况

用示例题进行掩码的说明：



划分子网实例示意图 01



划分子网实例示意图 02

	网络位	主机位			地址划分信息
默认IP类型	172.16	255		0	子网：172.16.0.0 掩码：255.255.0.0 主机：172.16.0.1-172.16.255.254
二进制说明	172.16	00000000		0	
掩码	255.255	0		0	/16
	网络位	主机位			地址划分信息
默认IP类型	172.16	子网位 255		0	
二进制说明	172.16	00000000		0	子网：172.16.0.0 掩码：255.255.192.0 主机：172.16.0.1-172.16.63.254
掩码	255.255	192		0	/18
二进制说明	172.16	01000000		0	子网：172.16.192.0 掩码：255.255.192.0 主机：172.16.64.1-172.16.127.254
掩码	255.255	192		0	/18
二进制说明	172.16	11000000		0	子网：172.16.192.0 掩码：255.255.192.0 主机：172.16.128.1-172.16.191.254
掩码	255.255	192		0	/18

划分子网实例示意图 03

- 1 运营商或者领导给我们一个IP地址加子网掩码我们必须要知道可配置的IP地址范围
- 2 116.63.0.10/29 网关：116.63.0.9
- 3 <https://www.36130.com/subnetmask/>
- 4 网关：116.63.0.9
- 5
- 6 116.63.0.10 255.255.255.248 网关 116.63.0.9 配置到哪个服务器上。

网络和IP地址计算器

输入IP	116	63	0	10	掩码位	29	计算	清空
可用IP	6							
掩码	255	255	255	248				
网络	116	63	0	8				
第一可用	116	63	0	9				
最后可用	116	63	0	14				
广播	116	63	0	15				

显示网络, 广播, 第一次和最后一个给定的网络地址
在网络掩码“位格式”也被称为CIDR格式 (CIDR=无类别域间路由选择)。

8. 网关

1 网关 (Gateway) 又称网间连接器, 就是一个网络连接到另一个网络的“关口”。

2

3 网关实质上是一个网络通向其他网络的IP地址。比如有网络A和网络B，网络A的IP地址范围为“192.168.1.1~192.168.1.254”，子网掩码为255.255.255.0；网络B的IP地址范围为“192.168.2.1~192.168.2.254”，子网掩码为255.255.255.0。在没有路由器的情况下，两个网络之间是不能进行TCP/IP通信的，即使是两个网络连接在同一台交换机(或集线器)上，TCP/IP协议也会根据子网掩码(255.255.255.0)判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信，则必须通过网关。如果网络A中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B的某个主机(如附图所示)。网络B向网络A转发数据包的过程。

4

5 所以说，只有设置好网关的IP地址，TCP/IP协议才能实现不同网络之间的相互通信。那么这个IP地址是哪台机器的IP地址呢？网关的IP地址是具有路由功能的设备的IP地址，具有路由功能的设备有路由器、启用了路由协议的服务器(实质上相当于一台路由器)、代理服务器(也相当于一台路由器)。

6

7

8 # ifconfig route netstat 命令属于net-tools网络工具包
9 ip add linux
10 ifconfig linux
11 ping linux windows
12 nslookup linux
13 route -n
14
15 tracert -d www.baidu.com windows
16

```
17 [root@oldboy:~]# traceroute -n
18 www.baidu.com
19
20 [root@oldboy ~]# route -n      # 查看网关
21 Kernel IP routing table
22 Destination      Gateway          Genmask
23             Flags Metric Ref  Use Iface
24 0.0.0.0          10.0.0.2      0.0.0.0
25             UG     0      0      0 eth0
26 10.0.0.0          0.0.0.0
27             255.255.255.0   U     0      0      0 eth0
28 169.254.0.0      0.0.0.0
29             255.255.0.0   U     1002   0      0 eth0
30
31 给网卡配置多个IP地址：临时重启失效  笔记
32 [root@oldboy ~]# ip add add 10.0.0.201/24
33 dev eth0
34 删除临时IP：
35 [root@oldboy ~]# ip address del
36 10.0.0.201/24 dev eth0
37
38 临时删除网关：
39 [root@oldboy ~]# ip route del 0/0 via
40 10.0.0.2
41 配置临时的网关：
42 [root@oldboy ~]# ip route add 0/0 via
43 10.0.0.2
44
45 #笔试题 给linux系统配置一个默认网关
46 vim /etc/sysconfig/network-scripts/ifcfg-
47 ens33
48 GATEWAY
```

```
39 [root@oldboy ~]#route add default gw
      10.0.0.3
40 [root@oldboy ~]#route del default gw
      10.0.0.3 # 删除默认网关
41
42 知识重点：
43 1.OSI七层模型
44 应用层
45 表示层
46 会话层
47 传输层
48 网络层
49 数据链路层
50 物理层
51 2.TCP/TP四层
52 应用层
53 主机到主机层
54 inter网
55 接入层
56
57 3.DNS解析流程
58
59 4.TCP三次握手
60 为什么要三次握手
61 5.TCP四次挥手
62
63 6.TCP11状态 笔记
64
65 7.IP地址/子网掩码 子网掩码决定了IP可用的数量
66
67
68
69
```

9. 抓包方式

抓包方式：wireshark抓包软件在Windows中使用

Linux抓包命令tcpdump是一个抓包工具，用于抓取互联网上传输的数据包

```
1      tcpdump是一个用于截取网络分组，并输出分组内容的
2      工具。凭借强大的功能和灵活的截取策略，使其成为类UNIX
3      系统下用于网络分析和问题排查的首选工具
4      tcpdump 支持针对网络层、协议、主机、网络或端口
5      的过滤，并提供and、or、not等逻辑语句来帮助你去掉无
6      用的信息
7
8
9
10
11
12
13
14
15
16
17
18
19
```

1 #常用选项

2 [root@oldboyedu ~]#yum -y install tcpdump

3

4 -i #监听哪一个网卡

5 -n #不把ip解析成主机名

6

7 -nn #不把端口解析成应用层协议

8 -c #指定抓包的数量

9 -S #不把随机序列和确认序列解析成绝对值

10 -w #将流量保存到文件中，文件中的信息是无法直接
11 查看的

12 -r #读取文件中的内容

13 -v #输出一个稍微详细的信息，例如在ip包中可以
14 包括ttl和服务类型的信息。

15 -vv #输出详细的报文信息。

16 -nnnvi ens33

17

18 #实例

19 企业中遇到无法远程连接拍错流程：IDC机房服务器 云服务
器

```
20 1.ping通
21 2.通过页面或者机房插显示器连接服务器抓包
22 tcpdump -nni eth0 port 12345
23 3.在公司windows电脑使用telnet连接测试
24 cmd窗口-->telnet 服务器IP地址 12345
25
26 结果：
27 1.如果服务端可以看到来源公网IP地址 说明服务端做的限制
28 2.如果服务端来源IP地址不是公司公网IP地址 则需要放行
   抓取到的公网(打电话解决)
29 3.如果服务端收不到任何信息，说明是公司网络问题
30
31 保存到文件中
32 [root@oldboy:~]# tcpdump -w 1.txt -nnvvi
   ens33 dst www.baidu.com
33 查看文件中的内容
34 [root@oldboy:~]# tcpdump -r 1.txt
35
36
37 1、默认启动
38
39 tcpdump -vv      #普通情况下，直接启动tcpdump将监
   视第一个网络接口上所有流过的数据包。
40
41 2、过滤主机
42
43 tcpdump -i eth1 host 192.168.1.1      #抓取
   所有经过eth1，目的或源地址是192.168.1.1的网络数据
44
45 tcpdump -i eth1 src host 192.168.1.1    #指定
   源地址，192.168.1.1
46
```

```
47 tcpdump -i eth1 dst host 192.168.1.1      #指定
      目的地址, 192.168.1.1
48
49 3、过滤端口
50
51 tcpdump -i eth1 port 80                  #抓取所有经过
      eth1, 目的或源端口是80的网络数据
52
53 tcpdump -i eth1 src port 80      #指定源端口
54
55 tcpdump -i eth1 dst port 80      #指定目的端口
56
57 4、协议过滤
58
59 tcpdump -i eth1 arp
60
61 tcpdump -i eth1 ip
62
63 tcpdump -i eth1 tcp
64
65 tcpdump -i eth1 udp
66
67 tcpdump -i eth1 icmp
68
69 #抓tcp某端口的数据包
70
71 tcpdump -i eth0 tcp port 21 -nn
72
73 5、常用表达式
74
75 非 : ! or "not" (去掉双引号)
76
77 且 : && or "and"
```

```
78
79 或 : || or "or"
80
81 #抓取所有经过eth1, 目的地址是192.168.1.254或
82 #192.168.1.200端口是80的TCP数
83 tcpdump -i eth1 '((tcp) and (port 80) and
84 ((dst host 192.168.1.254) or (dst host
85 192.168.1.200)))'
86
87 #抓取所有经过eth1, 目标MAC地址是
88 00:01:02:03:04:05的ICMP数据
89 tcpdump -i eth1 '((icmp) and ((ether dst
90 host 00:01:02:03:04:05)))'
91 #抓取所有经过eth1, 目的网络是192.168, 但目的主机不
92 是192.168.1.200的TCP数据
93 tcpdump -i eth1 '((tcp) and ((dst net
94 192.168) and (not dst host 192.168.1.200)))'
```

10. Linux常用网络命令

1. 网卡命令规则

```
1 CentOS-6之前基于传统的命名方式如: eth1, eth0....
2
3 CentOS-7提供了不同的命名规则, 默认是基于固件、拓
4 扑、位置信息来分配。这样做的优点是命名是全自动的、可
5 预知的, 缺点是比eth0、wlan0更难读。比如enp5s0
6
7 biosdevname和net.ifnames两种命名规范
```

```
6
7 #net.ifnames的命名规范为:
8
9     设备类型+设备位置+数字
10
11 #设备类型:
12
13     en 表示Ethernet
14
15     w1 表示WLAN
16
17     ww 表示无线广域网WWAN
18
19 #实际的例子:
20
21     eno1      #板载网卡
22
23     enp0s2    #pci网卡
24
25     ens33    #pci网卡
26
27     wlp3s0    #PCI无线网卡
28
29     wwp0s29f7u2i2    #4G modem
30
31     wlp0s2f1u4u1    #连接在USB Hub上的无线网卡
32
33 #biosdevname的命名规范为:
34
35     根据系统BIOS提供的信息对网络接口进行重命名。
36
37     em[1-N] #表示主板（嵌入式）NIC（对应机箱标签）
```

```
38
39      pci      #表示PCI插槽中的卡，端口1至N
40
41 实际的例子：
42
43      em1      #板载网卡
44
45      p3p4    #pci网卡
46
47      p3p4_1  #虚拟网卡
48
49 CentOS-7
50
51 默认内核参数(biosdevname=0 (de11服务器默认是1) ,
52      net.ifnames=1): 网卡名 "enp5s2"
53 biosdevname=1, net.ifnames=0: 网卡名 "em1"
54
55 biosdevname=0, net.ifnames=0: 网卡名 "eth0"
56 (最传统的方式,eth0 eth1)
57
58 #定义网卡命令规则
59 在安装系统时，选择安装选项，按tab键，在跳出的一行内
60 容后面添加net.ifnames=0 biosdevname=0
61
62 #命令行设置网卡名称规则
63 [root@q1s ~]# cd /etc/sysconfig/network-
64      scripts/ #修改网卡配置文件
65 [root@q1s network-scripts]# mv ifcfg-ens33
66      ifcfg-eth0
```

```
65 [root@q1s network-scripts]# sed -i  
66 "s#ens33#eth0#g" ifcfg-eth0  
66 [root@q1s ~]# vim /etc/sysconfig/grub #GRUB  
添加kernel参数  
67 GRUB_CMDLINE_LINUX="...net.ifnames=0  
biosdevname=0 quiet"  
68 [root@q1s ~]# grub2-mkconfig -o  
/boot/grub2/grub.cfg  
69 [root@q1s ~]# reboot #重启系统生效
```

2. 网卡配置文件详解

```
1 #动态ip  
2 [root@q1s ~]# cat /etc/sysconfig/network-  
scripts/ifcfg-eth0  
3 TYPE="Ethernet"  
4 PROXY_METHOD="none"  
5 BROWSER_ONLY="no"  
6 BOOTPROTO="dhcp"  
7 DEFROUTE="yes"  
8 IPV4_FAILURE_FATAL="no"  
9 IPV6INIT="yes"  
10 IPV6_AUTOCONF="yes"  
11 IPV6_DEFROUTE="yes"  
12 IPV6_FAILURE_FATAL="no"  
13 IPV6_ADDR_GEN_MODE="stable-privacy"  
14 NAME="eth0"  
15 UUID="fb32c09d-5a9f-40b9-852b-0f44ff2202ed"  
16 DEVICE="eth0"  
17 ONBOOT="yes"  
18  
19 #静态ip
```

```
20 [root@q1s ~]# cat /etc/sysconfig/network-
21 scripts/ifcfg-eth0
22 TYPE="Ethernet"
23 BOOTPROTO="static"
24 NAME="eth0"
25 DEVICE="eth0"
26 ONBOOT="yes"
27 IPADDR="10.0.0.88"
28 NETMASK="255.255.255.0"
29 GATEWAY="10.0.0.254"
30 DNS1="223.5.5.5"
31 DNS2="223.6.6.6"
32
33 #详解:
34
35 TYPE=Ethernet          #网卡类型，一般是Ethernet，还有其他的如bond, bridge
36
37 BOOTPROTO=dhcp          #获取IP地址的方式，启动的协议，获取配置的方式。
38
39
40
41 DEFROUTE=yes          #是否设置默认路由，若为yes则可以在该文件通过PREFIX这个参数来设置子网掩码
42
43 PEERDNS=yes          #yes表示由DHCP来获取DNS，no表示/etc/resolv.conf来控制，默认为yes。
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1088
1089
1090
1091
1092
1093
1094
1095
1096
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1188
1189
1190
1191
1192
1193
1194
1195
1195
1196
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1290
1291
1292
1293
1294
1295
1295
1296
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1395
1395
1396
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1488
1489
1490
1491
1492
1493
1494
1495
1495
1496
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1588
1589
1590
1591
1592
1593
1594
1595
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1688
1689
1690
1691
1692
1693
1694
1695
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1788
1789
1790
1791
1792
1793
1794
1795
1795
1796
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1888
1889
1890
1891
1892
1893
1894
1895
1895
1896
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1988
1989
1990
1991
1992
1993
1994
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2088
2089
2090
2091
2092
2093
2094
2095
2095
2096
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2188
2189
2190
2191
2192
2193
2194
2195
2195
2196
2197
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2217
2218
2219
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2238
2
```

```
45 no: 不修  
改/etc/resolv.conf中的DNS  
46  
47 NAME=eth0 #这个参数对应的值是网卡名，是  
给用户看的  
48  
49 UUID=... #通用唯一识别码，若vmware克  
隆的虚拟机无法启动网卡可以去除此项  
50  
51 DEVICE=eth0 #系统逻辑设备名  
52  
53 ONBOOT=yes #开机启动时是否激活网卡设备，  
centos7装完网卡后默认设置成no  
54  
55 HWADDR=... #以太网硬件地址，mac地址）。  
若是vmware克隆的虚拟机无法启动网卡，也要改这个。  
56  
57 NM_CONTROLLED=yes #是否通过NetworkManager管  
理网卡设备  
58  
59 IPADDR=... #设置网卡对应的IP地址，网络  
服务启动，网卡激活后会自动将该地址配置到网卡上  
60 前提（BOOTPROTO=static）而  
不是dhcp  
61  
62 PREFIX=24 #子网掩码长度，不要这么写  
PREFIX=255.255.255.0  
63  
64 NETMASK=255.255.255.0 #生产环境中一般用这种方  
式指定子网掩码  
65  
66 GATEWAY=10.0.0.254 #该网卡配置的IP对应的网关  
(默认路由)
```

```
67 若主机是多网卡设备，该参数只
    能在一个网卡配置文件里面出现，一台主机只有一个默认路
    由
68
69 DNS1=... #主DNS，若这里设置了值，则会
    优先于/etc/resolv.conf中设置的DNS服务器的地址
70 需要和“PEERDNS=no”配合使用
71
72 DNS2=... #次dns
73
74 USERCTL=no #USERCTL=yes/no是否允许非
    root用户控制该设备
75
76 IPV6INIT=no #是否启用IPV6
77
78 BROADCAST=... #广播地址
79
80 PROXY_METHOD=none #代理方式，一般不用这个参数
81
82 BROWSER_ONLY=no #没有什么用。
83
84 #修改网卡配置文件的方法
85
86 vim /etc/sysconfig/network-scripts/ifcfg-
    eth0
87
88 nmcli #需要开启NetworkManger
```

3. 网络管理命令

ping

1 ping命令主要的功能是用来检测网络的连通情况和分析网络速度。

```
2
3 #常用选项
4
5      -t      #持续ping, 不中断。不加该选项只ping4
6      个包。
7      -c      #ping的包数, 默认是4个。
8      -w      #多长时间ping一次。
9      -f      #极速ping。
10 windows: ping不通不能表示服务器不能访问 可能服务器
11 禁止了ICMP协议(禁ping)
12 C:\Users\oldboy-lidao996>ping -n 2
13 www.baidu.com
14 正在 Ping www.a.shifen.com [110.242.68.3] 具
15 有 32 字节的数据:
16 来自 110.242.68.3 的回复: 字节=32 时间=11ms
17 TTL=52
18 来自 110.242.68.3 的回复: 字节=32 时间=12ms
19 TTL=52
20 110.242.68.3 的 Ping 统计信息:
21 数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0%
22 丢失),
23 往返行程的估计时间(以毫秒为单位):
24 最短 = 11ms, 最长 = 12ms, 平均 = 11ms
25
26 centos:
27 [root@oldboyedu ~]#ping -c2 -w1
28 www.baidu.com
29 PING www.a.shifen.com (110.242.68.4) 56(84)
30 bytes of data.
```

```
25 64 bytes from 110.242.68.4 (110.242.68.4):  
    icmp_seq=1 ttl=128 time=16.3 ms  
26 64 bytes from 110.242.68.4 (110.242.68.4):  
    icmp_seq=2 ttl=128 time=11.1 ms  
27  
28 -c     ping的个数  
29 -w1  延时1秒返回请求  
30
```

nc

```
1 nc是netcat的简写，有着网络界的瑞士军刀美誉。因为它短  
    小精悍、功能实用，被设计为一个简单、可靠的网络工具  
2  
3 #常用选项  
4  
5     -l      #用于指定nc将处于侦听模式。  
6     -u      #指定nc使用UDP协议，默认为TCP  
7     -v      #输出交互或出错信息，新手调试时尤为有用  
8     -w      #超时秒数，后面跟数字  
9     -z      #表示zero，表示扫描时不发送任何数据
```

nmap

1 Nmap即网络映射器对Linux系统/网络管理员来说是一个开源且非常通用的工具。Nmap用于在远程机器上探测网络，执行安全扫描，网络审计和搜寻开放端口。

2

3 #常用选项

4

5 -p #指定端口号

6 -p22 #单个端口

7 -p22,80 #多个端口

8 -p1-1000 #1到1000之间的端口

9

10

11 企业案例：

12 写一个脚本 探测自己所有的服务器上开放的服务以及端口
并且计算一些每个服务占用所有服务的百分比

13 100台服务器

telnet

```
1 一种远程登录的工具。同样可以检查某个主机是否开启某个
2 端口
3 默认端口23
4 #用法 主要功能链接路由器、交换机 telnet
5 192.168.13.1
6
7
8 Connecting to 10.0.0.99:22...
9 Connection established.      # 连接成功 说明22端
10 口开启
11 To escape to local shell, press
12 'Ctrl+Alt+]'.
13 SSH-2.0-OpenSSH_7.4
```

netstat

```
1 打印网络连接、路由表、tcp11种状态。
2 查看当前系统中运行了哪些服务端口
3 #常用选项
4     -l      #只显示监听套接字。
5     -n      #不做名字解析
6     -t      #显示tcp端口
7     -u      #显示udp端口
8     -p      #显示pid和程序名字
9     -r      #显示路由表
10    -a      #显示所有的套接字
11
12 netstat -tnulp
```

ss

```
1 跟netstat命令差不多。
2
3 #常用选项
4 -l      #只显示监听套接字。
5 -n      #不做名字解析
6 -t      #显示tcp端口
7 -u      #显示udp端口
8 -p      #显示pid和程序名字
9 -r      #解析主机名
10 -a     #显示所有的套接字
11
```

tracert

```
1 (windows) 路由跟踪（检查你与目标之间每个路口是否畅通）
2
3 #常用选项
4
5 -d      #禁止把IP解析为对应的域名（主机名）
6 C:\Users\oldboy-lidao996>tracert -d
7 www.baidu.com
8 通过最多 30 个跃点跟踪
9 到 www.a.shifen.com [110.242.68.3] 的路由：
10
11 1      1 ms      1 ms      2 ms  192.168.11.1
12 2      2 ms      <1 毫秒    5 ms  192.168.1.1
13 3      4 ms      3 ms      3 ms
14               221.218.208.1
15 4      2 ms      8 ms      6 ms
16               61.148.162.57
17 5      3 ms      7 ms      4 ms  202.106.34.1
```

```
16 6 4 ms 3 ms 3 ms 202.96.12.1
17
18 DNS流程：
19 浏览器缓存-->HOSTS-->windows缓存-->LDNS-->根
20
21 查看windows缓存：
22 ipconfig/displaydns
23 C:\Users\oldboy-lidao996>ipconfig/flushdns
24
25 windows IP 配置
26
27 已成功刷新 DNS 解析缓存。
28
29
30 cmd---->mstsc 调出远程桌面
```

traceroute

```
1 路由跟踪（检查你与目标之间每个路口是否畅通）
2
3 #常用选项
4
5 -n 禁止把IP解析为对应的域名（主机名）
6 在Linux系统中使用：
7 [root@oldboyedu ~]#traceroute -n -I
www.baidu.com
8 traceroute to www.baidu.com (110.242.68.4),
30 hops max, 60 byte packets
9 1 10.0.0.2 0.216 ms 0.176 ms 0.100 ms
10 2 192.168.11.1 25.034 ms 24.795 ms
24.615 ms
11 3 192.168.1.1 22.107 ms 21.941 ms
21.748 ms
```

iftop

```
1 | iftop界面说明:  
2 |  
3 | 界面上面显示的是类似刻度尺的刻度范围，为显示流量图形  
4 | 的长条作标尺用的。  
5 | 中间的<= =>这两个左右箭头，表示的是流量的方向。  
6 |  
7 | TX: 发送流量  
8 | RX: 接收流量  
9 | TOTAL: 总流量  
10 | Cumm: 运行iftop到目前时间的总流量  
11 | peak: 流量峰值  
12 | rates: 分别表示过去 2s 10s 40s 的平均流量  
13 |  
14 | #常用选项  
15 |  
16 | -i      #设定监测的网卡  
17 |  
18 | -B      #以bytes为单位显示流量(默认是bits)  
19 |  
20 | -n      #使host信息默认直接都显示IP  
21 |  
22 | -P      #使host信息及端口信息默认就都显示  
23 |  
24 | -m      #设置界面最上边的刻度的最大值，刻度分五个大  
25 | 段显示  
26 | 按q退出监控。  
27 |  
28 | yum -y install dstat  
29 | dstat -nf
```

```
30
31
32
33
34 网络重点：
35 1. 网络常用命令
36 ping
37 ip add
38 route -n
39 ifconfig
40 nslookup
41 tcpdump
42 iftop
43 iotop
44 netstat -tnulp
45 ss -an|grep tcp
46 telnet
47
48 tracert
49 nmap
50
51 windows
52 ping
53 nslookup
54 mstsc
55 cmd
56 ipconfig/all
57 ipconfig/flushdns
58 ipconfig/displaydns
59
60 2. OSI七层模型
61
62 3. TCP三次握手
```

63
64 4.TCP四次挥手
65
66 5.DNS解析流程
67
68 6.子网掩码决定IP可用数量
69
70 7.静态路由动态路由理解
71
72
73
74 #下次内容 开始二阶段架构
75 #周一 综合考试