[网络知识 1](#_Toc930597309)

[TCP/IP协议 1](#_Toc1586230932)

[IP地址 1](#_Toc490821684)

[配置IP地址 2](#_Toc1703146569)

[网关和DNS 3](#_Toc10514437)

[常见的协议 （9大协议） 4](#_Toc248578117)

[OSI七层模型 4](#_Toc1312996860)

# 网络知识

## TCP/IP协议

1、TCP/IP通信协议是目前最完整、最被广泛支持的通信协议，它可以让不同网络架构、不同操作系统的计算机之间通信，是Internet的标准通信协议

2、主机与主机之间通信三个要素

IP地址（IP address）

子网掩码（subnet mask）

IP路由（IP router）

## IP地址

1、 作用：用来标识一个节点的网络地址

2、 组成：32位，以4个十进制数来表示，之间用 . 隔开

网络位+主机位

127.0.0.1 :表示特殊的ip地址（永远代表自己）

3、 分类：

A 1 ~ 126 网+主+主+主

B 128 ~ 191 网+网+主+主

C 192 ~ 223 网+网+网+主

D 224 ~ 239 组播(多播)

E 240 ~ 254 科研

4、默认子网掩码

A 类 255.0.0.0

B类 255.255.0.0

C 类 255.255.255.0

5、公有IP地址和私有IP地址

公有地址，也可称为公网地址，通过它直接访问因特网，它是广域网范畴内的。

私有地址，也可称为专网地址，专门为组织机构内部使用，它是局域网范畴内的，出了所在局域网是无法访问因特网的。

私有地址范围：

A类 10.0.0.1 ~ 10.255.255.254

B类 172.16.0.1 ~ 172.31.255.254

C类 192.168.0.1 ~ 192.168.255.254

6、网关

就是一个网络连接到另一个网络的“关口”

通常是一台路由器

## 配置IP地址

### windows配置ip

– 右击桌面网络 ---->属性 ---->更改适配器设置

– 双击“本地连接” ----> 属性

– 双击“Internet协议版本4(TCP/IPv4)”

– 配置完成后,单击“确定”完成

自动配置ip地址，网络有DHCP服务器 DHCP协议

手工配置ip地址

命令的方式： ipconfig

查看IP地址的命令 ipconfig （windows)

操作步骤:

在cmd中运行命令查看

ipconfig /all

测试通信： 一次 ping 指的双向的 有去有回 （关闭两台虚拟机的防火墙）

### linux配置ip:

**临时设置:** ifconfig eth0 192.168.1.1

ifconfig: 列出已激活的网卡连接信息 默认第一张网卡的名为 eth0

**永久配置1: 修改配置文件**

vim /etc/sysconfig/network-scripts/ifcfg-eth0 #网卡配置文件

PROXY\_METHOD="none"

BROWSER\_ONLY="no"

DEFROUTE="yes"

NAME="eth0"

DEVICE="eth0"

ONBOOT="yes"

IPV6INIT="no"

IPV4\_FAILURE\_FATAL="no"

NM\_CONTROLLED="no"

TYPE="Ethernet"

BOOTPROTO="none" //也可以是dhcp,后面几行就不需要了

IPADDR="192.168.1.11"

PREFIX=24

GATEWAY="192.168.1.254"

**永久配置2: networkmanager**

a.查看识别的网卡名称 #nmcli connection show

b.配置ip地址 子网掩码 网关地址

# nmcli connection modify 'System eth0' ipv4.method manual \

ipv4.addresses '172.25.0.100/24 connection.autoconnect yes

[root@A ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0

c.激活配置

[root@A ~]# nmcli connection up 'System eth0'

[root@A ~]# ifconfig #查看ip地址

[root@A ~]# route #查看网关地址 gateway

Nmcli connection reload ifcfg-eth3 重新加载

ifconfig -a 查看所有网卡

**配置IPv6地址**

IPv4地址： 32个二进制 点 分隔 4个部分 十进制表示

IPv6地址： 128个二进制 冒号 分隔 8 个部分 16进制表示

配置:

# nmcli connection show

# nmcli connection modify 'System eth0' ipv6.method manual

ipv6.addresses 2003:ac18::305/64 connection.autoconnect yes

# nmcli connection up 'System eth0'

查看: # ifconfig | head -4

# ping6 2003:ac18::305

## 网关和DNS

网关：从一个网络连接到另一个网络的“**关口**” (不同的网络之间的通信)

DNS 域名解析服务器： **解析域名** 将域名解析为IP地址

访问Web网站： 客户端 www.qq.com 腾讯的Web服务器： 提供页面的内容

### 配置永久DNS服务器地址

DNS服务器地址永久配置文件:/etc/resolv.conf

[root@student ~]# echo nameserver 172.25.254.254 > /etc/resolv.conf

[root@student ~]# nslookup server0.example.com #测试DNS解析

Server: 172.25.254.254

Address: 172.25.254.254#53

Name: server0.example.com

Address: 172.25.0.11

## 常见的协议 （9大协议）

**默认端口**

**http 超文本传输协议 80**

**https 安全的超文本传输协议 443**

**ftp 文件传输协议 21**

**tftp 简单的文件传输协议 69**

**telnet 远程管理协议 23**

**dns 域名解析协议 53**

**smtp 邮件协议 25**

**pop3 收邮件协议 110**

**snmp 简单的管理协议 161**

**SSH 远程管理协议 22**

## OSI七层模型

网络协议与标准

1、协议：一组控制数据通信的规则，协议的三要素：语法、语义，同步。

2、标准：一致同意的规则可以理解为标准

ISO（国际标准化组织）在网络通信中创建了OSI（开放系统互联）模型。

ANSI（美国国家标准化局）

ITU-T（国际电信联盟-电信标准部）

IEEE（电气和电子工程师学会）

按照网络规模和使用范围分类为

WAN:广域网

LAN:局域网

**OSI是一个开放式体系结构，它规定将网络分为七层**

**应用层：**

网络服务与最终用户的一个接口（上层数据）

HTTP、https、FTP、TFTP、SMTP 、pop3、SNMP、DNS 、telnet

**表示层：**

数据的表现形式，如加密、压缩。（上层数据）

**会话层：**

建立、管理、中止会话，例如断点续传。（上层数据）

**传输层：**

定义传输数据的协议端口号，以及流控和差错校验，实现了程序与程序的互连，可靠与不可靠的传输。

TCP、UDP

**网络层：**

进行逻辑地址寻址，实现不同网络之间的通信，定义了IP地址，为数据传输选择最佳路径，路由器工作在网络层。

ICMP、IGMP、IP、ARP、RARP

**数据链路层：**

建立逻辑连接、进行硬件地址寻址、差错校验等功能、通过MAC地址实现数据的通信，帧包装、帧传输、帧同步。交换机工作在数据链路层。

**物理层：**

建立、维护、断开物理连接，定义了接口及介质，实现了比特流的传输。（比特流运输）

数据在传输的过程中从上层入下层进行封装，对于接收方从底层到顶层进行解封装。（MAC头部-IP头部-TCP头部-上层数据）

**PDU（协议数据单元**）

传输层 段 segment

网络层 报文 packet 包

数据链路层 帧 frame

物理层 比特 bit

**相应层次的设备**

应用层 计算机

传输层 防火墙

网络层 路由器

数据链路层 交换机

物理层 网卡,中继器

能放大信号

延长网络传输距离

只包含有一个输入端口和一个输出端口，所以只能接受和转发数据流

成本低

### 物理层

一、接口

以太网接口：

RJ-45水晶头（常规网线接口）

RJ-11水晶头，电话线的接头

光纤接口：无源组件

FC 、ST、SC

LC 窄体方形光纤接头（目前主流）

MT-RJ

二、双绞线（网线）

1）双绞线分类：

屏蔽双绞线（STP）线外包裹一层金属网膜，用于电磁环境非常复杂的工业环境中

非屏蔽双绞线 （UTP）

2）双绞线标准与分类 ：

类型 传输速率

Cat5 五类线 100Mbps

Cat5e超五类 100Mbps衰减更小，串扰更少，性能优于5类线 (可以传1000Mbps）

Cat6 六类线 1000Mbps（1Gbps）

Cat7 七类线 10000Mbps（10Gbps）

三、双绞线的连接规范

1）线序

T568A:白绿、绿、白橙、蓝、白蓝、橙、白棕、棕

T568B:白橙、橙、白绿、蓝、白蓝、绿、白棕、棕

1、2发送,3、6接收(这4根线发挥作用)，其他4根一般不被使用.超5类 cat5e 传输1000Mbps时，8根线全部用到

2）线缆的连接：

标准网线（**直连线**或直通线）：两边都是同一线序，都是T568A或者都是T568B，有2种类型，默认使用T568B

**交叉网线**：两边为不同的线序，一边是T568A，另一头是T568B

!!!!!!!凡是与交换机相连的都使用直通线

!!!!!!!其他都用交叉线

特例：交换机与交换机相连使用交叉或直连线，一般用交叉线

**全反线** ：不用于以太网的连接，主要用于计算机的串口和路由器或交换机的console（控制口）相连

### 数据链路层

功能

- 数据链路的建立、维护与拆除

- 帧包装、帧传输、帧同步

- 帧的差错恢复

- 流量控制

**MAC地址:**用来识别一个以太网上的某个单独的设备或一组设备

MAC地址长度48位(6个字节)，前24位代表厂商，后24位代表网卡编号，

MAC 地址的第8位为0时表示该MAC地址为单播地址，为1时表示组播地址。48位都为1表示广播地址。

一般使用16进制表示：由12位组成，广播地址为ff-ff-ff-ff-ff-ff

Ipconfig /all查看MAC地址

注：一块物理网卡的地址一定是一个单播地址，也就是第8位一定为0

帧校验序列（FCS）：从目的地址开始到数据结束这部分的校验和。

类型/长度：用来标识上层协议的类型或后续数据的字节长度。

**交换机**

1、交换机是用来连接局域网的主要设备， 交换机分割冲突域，实现全双工通信

2、交换机的工作原理.维护mac地址表

初始状态->根据源MAC地址学习->除源端口外的端口广播未知数据帧->接收方回应->交换机实现单播通信（转发）->记录目标mac地址

mac表更新：1. 老化时间300秒

2. 交换机对应端口的MAC 地址发生变化时

总结为：

- 学习：mac地址表是交换机通过学习接受的数据帧的源mac地址来形成

- 广播：除源端口外的其他所有端口广播未知数据帧

- 转发：接收方回应，交换机根据mac地址表单播转发数据帧

- 更新：老化时间300秒，交换机对应端口的MAC 地址发生变化时交换机将mac地址重新学习到新的端口

3、交换机以太网接口双工模式

单工：两个数据站之间只能沿单一方向传输数据

半双工：两个数据站之间可以双向数据传输，但不能同时进行

全双工：两个数据站之间可双向且同时进行数据传输

4、冲突与广播域

广播域指接收同样广播消息的节点的集合

交换机分割冲突域，但是不分割广播域，即交换机的所有端口属于同一个广播域

交换机的每个端口访问另一个端口时，都有一条专有的线路，不会产生冲突

5. VLAN

虚拟局域网

广播控制、安全性、带宽利用、延迟

分割广播域

6. trunk中继链接

1、作用：实现交换机之间的单一链路传递多个vlan的信息

2、链路类型：

1）接入链路: access 可以承载1个 vlan

2）中继链路：trunk可以承载多个 vlan

3、vlan的标识

1）ISL(cisco私有的标记方法)

ISL外部封装头部26个字节，尾部4个字节共30字节

2）IEEE 802.1q(公有的标记方法)

内部封装在标准以太网帧内插入了4个字节，其中12位vlan标识。

4、ISL和802.1Q 的异同

相同点:都是显示了VLAN的信息

不同点:

IEEE 802.1Q是公有的标记方式，ISL是Cisco私有的

ISL采用外部标记的方法，802.1Q采用内部标记的方法

ISL标记的长度为30字节，802.1Q标记的长度为4字节

7. EthernetChannel（以太网通道）

以太通道为交换机提供了端口捆绑的技术，允许两个交换机通过两个或多个端口进行连接，同时传输数据，以提供更高的带宽

1、功能：多条线路负载均衡，带宽提高

容错，当一条线路失效时，其他线路通信，不会丢包

参与捆绑的端口必须属于同一个vlan,如果是在中继模式下，要求所有参加捆绑的端口都配置成中继模式。如果参与捆绑的端口的物理参数设置必须相同，应该有同样的速度和全/半双工模式设置

### 网络层

路由器原理及静态路由

1、路由

跨越从源主机到目标主机的一个互联网络来转发数据包的过程

2、路由表

路由器根据路由表做路径选择

3、路由表的获得

1）、直连路由：配置IP地址，端口UP状态，形成直连路由。

2）、非直连网段：需要静态路由或动态路由，将网段添加到路由表中。

4、静态路由

1）、特点：

由管理员手工配置的，是单向的，因此需要在两个网络之间的边缘路由器上需要双方对指，否则就会造成流量有去无回，缺乏灵活性，适用于小型网络。

2)、配置

全局模式：

ip route 目标网络ID 子网掩码 下一跳IP

3)、浮动路由

配置浮动静态路由，需设置管理距离大于1，从而成为备份路由，实现链路备份的作用。

5. 缺省路由（默认路由）

缺省路由是一种特殊的静态路由.简单地说,缺省路由就是在没有找到任何匹配的具体路由条目的情况下才使用的路由，适用于只有一个出口的末节网络（比如企业的网关出口），优先级最低，可以做为其他路由的补充。

全局:ip route 0.0.0.0 0.0.0.0 下一跳

代表任意网络ID 代表任意子网掩码

查看路由表

特权：show ip route

C直连路由

S静态路由

S\*默认路由

**三层交换技术:**

1、作用

使用三层交换技术实现VLAN间通信

三层交换=二层交换+三层转发

2、基于CEF 的快速转发

主要包含两个转发用的信息表：

1）转发信息库（FIB）：FIB类似于路由表，包含路由表中转发信息的镜像。当网络的拓扑发生变化时，路由表将被更新，而FIB也将随之变化。

2）邻接关系表：每个FIB条目，邻接关系表中都包含相应的第2层地址。

3、虚拟接口（SVI）

三层交换机上配置的VLAN接口为虚接口

6. 动态路由

a、动态路由特点

减少了管理任务

占用了网络带宽

b路由协议分类

1、按应用范围的不同，路由协议可分为两类：

1）在一个AS内的路由协议称为[内部网关协议](http://baike.baidu.com/view/706465.htm" \t "_blank)（interior gateway protocol），正在使用的[内部网关路由协议](http://baike.baidu.com/view/4217560.htm" \t "_blank)有以下几种：RIP-1，RIP-2，IGRP，EIGRP，IS-IS和OSPF。

2）AS之间的路由协议称为[外部网关协议](http://baike.baidu.com/view/543338.htm" \t "_blank)（exterior gateway protocol）。

外部网关协议（External Gateway Protocol，EGP，也叫域 间路由协议）。域间路由协议有两种：外部网关协议（EGP）和边界网关协议（BGP）

注：AS自治系统（Autonomous System，指一个[互连网络](http://baike.baidu.com/view/545553.htm" \t "_blank)，就是把整个Internet划分为许多较小的网络单位，这些小的网络有权自主地决定在本系统中应采用何种路由协议）

3）以情况下，需要使用BGP：

· 当你需要从一个AS发送[流量](http://baike.baidu.com/view/66422.htm" \t "_blank)到另一个AS时；

2、按照路由执行的算法动态路由协议的分类

1）距离矢量路由协议

依据从源网络到目标网络所经过的路由器的个数选择路由

RIP、IGRP

链路状态路由协议

综合考虑从源网络到目标网络的各条路径的情况选择路由

OSPF、IS-IS

RIP路由协议

RIP是距离-矢量路由选择协议

RIP度量值为跳数 ，最大跳数为15跳，16跳为不可达

**OSPF**协议

Open Shortest Path First ( 开放式最短路径优先）

OSPF区域

为了适应大型的网络，OSPF在AS内划分多个区域

每个OSPF路由器只维护所在区域的完整链路状态信息

区域ID

区域ID可以表示成一个十进制的数字

也可以表示成一个IP

骨干区域Area 0

负责区域间路由信息传播

TTL 值 数据包的生命值，每过一个路由器生命之减一Arp 全称 地址解析协议 将ip地址解析为mac地址

### 网络协议

Arp -a 查看arp缓存的mac地址

ICMP 协议 ping是该协议的工具

Windows

Ping -t 持续测试网络

-l 1000 修改ping包大小

Linux中

Ping -c 5 修改ping次数

-s 修改ping包大小

**TCP协议**

三次握手建立连接，SYN-》SYN&ACK-》ACK

四次握手断开连接 FIN&ACK -》ACK， FIN&ACK-》ACK

常用协议 FTP，TELNET，SMTP，DNS，HTTP

**UDP**

TFTP,DNS,NTP,RPC