1 、 OSI （ Open System Interconnect ）：开放系统互联，是一个七层的计算机网络模型，分别为：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

TCP/IP （ Transmission Control Protocol/Internet Protocol ）：传输控制协议 / 因特网互联协议，是一个四层的计算机网络模型，分别为：网络接口层、网络层、传输层和应用层。结合 OSI 和 TCP/IP 产生了一个五层结构，分别为：物理层、数据链路层、网络层、传输层和应用层。 Internet 就是采用的 TCP/IP 协议。

2 、集线器工作在 OSI 模型的物理层，网卡工作在 OSI 模型的物理层，交换机工作在数据链路层，路由器工作在网络层。

3 、机器 A 的 IP 地址为 202.96.128.130 ， 子网掩码为 255.255.255.128 ， 则该 IP 地址的网络号为 202.96.128(利用 IP 地址和子网掩码求与运算) ， 主机号为 130 。

4 、 ARP 是地址解析协议，简单语言解释一下工作原理。

答：

（ 1 ）首先，每个主机都会在自己的 ARP 缓冲区中建立一个 ARP 列表，以表示 IP 地址和 MAC 地址之间的对应关系。

（ 2 ）当源主机要发送数据时，首先检查 ARP 列表中是否有对应 IP 地址的目的主机的 MAC 地址，如果有，则直接发送数据，如果没有，就向本网段的所有主机发送 ARP 数据包，该数据包包括的内容有：源主机 IP 地址，源主机 MAC 地址，目的主机的 IP 地址。

（ 3 ）当本网络的所有主机收到该 ARP 数据包时，首先检查数据包中的 IP 地址是否是自己的 IP 地址，如果不是，则忽略该数据包，如果是，则首先从数据包中取出源主机的 IP 和 MAC 地址写入到 ARP 列表中，如果已经存在，则覆盖，然后将自己的 MAC 地址写入 ARP 响应包中，告诉源主机自己是它想要找的 MAC 地址。

（ 4 ）源主机收到 ARP 响应包后。将目的主机的 IP 和 MAC 地址写入 ARP 列表，并利用此信息发送数据。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败。

广播发送 ARP 请求，单播发送 ARP 响应。

5 、 DNS （ Domain Name System ）域名系统，简单描述其工作原理。

答：当 DNS 客户机需要在程序中使用名称时，它会查询 DNS 服务器来解析该名称。客户机发送的每条查询信息包括三条信息：包括：指定的 DNS 域名，指定的查询类型， DNS 域名的指定类别。基于 UDP 服务，端口 53. 该应用一般不直接为用户使用，而是为其他应用服务，如 HTTP ， SMTP 等在其中需要完成主机名到 IP 地址的转换。

6 、 TCP 和 UDP 的区别?

答： TCP 提供面向连接的、可靠的数据流传输，而 UDP 提供的是非面向连接的、不可靠的数据流传输。 TCP 传输单位称为 TCP 报文段， UDP 传输单位称为用户数据报。 TCP 注重数据安全性， UDP 数据传输快，因为不需要连接等待，少了许多操作，但是其安全性却一般。

7 、网关的作用?

答：通过它可以访问外网。

8 、 ipconfig 的作用是什么?

答：显示当前 TCP/IP 配置的信息。

9 、运行 net share 返回的结果是什么?

答：列出共享资源相关信息。

10 、 net use 和 net user 分别指什么?

答： net user 是对用户进行管理，如添加删除网络使用用户等。

net use 是对网络设备进行管理。

11 、如何查看当前系统开放的服务?

答：在命令提示符下执行 net services 命令。 Windows 下是用 net start

12 、除以上的命令，列出一些其他的命令?

答： taskkill ：用于结束至少一个进程

tasklist ：用于显示在本地或远程计算机上运行的所有进程

net view ：显示计算机列表

netstat ：显示网络连接、路由表和网络接口信息

ftp ：

telnet ：

13 、关掉以下服务会出现什么情况?

答：关掉 Automatic Updates ：则不能自动更新

关掉 Plug and Play ：则会导致 USB 不能使用

关掉 Remote Registry Service ：远程用户不能修改计算机上的注册表设置

关掉 Computer Browser ：则会无法维护网络上计算机的最新列表以及提供这个列表给请求的程序。

14 、端口及对应的服务？

答：

服务	端口号	服务	端口号
FTP	21	SSH	22
telnet	23	SMTP	25
Domain(域名服务器)	53	HTTP	80
POP3	110	NTP （网络时间协议）	123
MySQL 数据库服务	3306	Shell 或 cmd	514
POP-2	109	SQL Server	1433
SNMP			

15 、 ICMP 协议？

答： ICMP 是 Internet Control Message Protocol ，因特网控制报文协议。它是 TCP/IP 协议族的一个子协议，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、路由器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。 ICMP 报文有两种：差错报告报文和询问报文。

16 、 TFTP 协议？

答： Trivial File Transfer Protocol ，是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

17 、 HTTP 协议？

答： HTTP 超文本传输协议，是一个属于应用层的面向对象的协议，由于其简捷、快速的方式，适用于分布式超媒体信息系统。

18 、 DHCP 协议？

答：动态主机配置协议，是一种让系统得以连接到网络上，并获取所需要的配置参数手段。

19 、详细解释一下 IP 协议的定义，在哪个层上面，主要有什么作用？ TCP 和 UDP 呢？

答： IP 协议是网络层的协议，它是为了实现相互连接的计算机进行通信设计的协议，它实现了自动路由功能，即自动寻径功能。 TCP 是传输层的协议，它向下屏蔽 IP 协议的不可靠传输的特性，向上提供一种面向连接的、可靠的点到点数据传输。 TCP 在可靠性和安全

性上等更有保证。 UDP 也是传输层协议，它提供的是一种非面向连接的，不可靠的数据传输，这主要是有些应用需要更快速的数据传输，比如局域网内的大多数文件传输都是基于 UDP 的。UDP 在传输速率上更快，开销更小。

20 、请问交换机和路由器分别的实现原理是什么？分别在哪个层次上面实现的？
答：交换机用于局域网，利用主机的 MAC 地址进行数据传输，而不需要关心 IP 数据包中的 IP 地址，它工作于数据链路层。路由器识别网络是通过 IP 数据包中 IP 地址的网络号进行的，所以为了保证数据包路由的正确性，每个网络都必须有一个唯一的网络号。路由器通过 IP 数据包的 IP 地址进行路由的（将数据包递交给哪个下一跳路由器）。路由器工作于网络层。由于设备现在的发展，现在很多设备既具有交换又具有路由功能，两者的界限越来越模糊。

21 、 Internet 上保留了哪些 IP 地址用于内部？
答： 10.0.0 .0 172.16. 到 172.31 192.168.0. 到 192.168.255 。

22 、 ipconfig/all 用于查看申请的本机 IP 地址
ipconfig/release 用于释放 IP
ipconfig/renew 用于重新向 DHCP 服务器申请 IP 。

23 、 ADSL 使用的是频分多路复用技术。

24 、网桥的作用
答：网桥是一个局域网与另一个局域网之间建立连接的桥梁。

25 、防火墙的端口防护是指？
答：指通过对防火墙的端口开关的设置，关闭一些非必需端口，达到一定安全防护目的的行为。

26 、 IP 数据包的格式？ TCP 和 UDP 数据报的格式？及头部常见的字段？
答：
（ 1 ）一个 IP 数据报由**首部** 和**数据** 两部分组成。首部由**固定部分和可选部分** 组成。**首部的固定部分有 20 字节** 。可选部分的长度变化范围为 1—— 40 字节。固定部分的字段：

字段名	位数（ bit ）	字段名	位数

版本	4 Ipv4	首部长度	4 （表示的最大数为 15 个单位，一个单位表示 4 字节）
服务类型	8 以前很少用	总长度	16 （首部和数据部分的总长度，因此数据报的最大长度为 65535 字节，即 64KB ，但是由于链路层的 MAC 都有一定的最大传输单元，因此 IP 数据报的长度一般都不会有理论上的那么大，如果超出了 MAC 的最大单元就会进行分片）
标识	16 （相同的标识使得分片后的数据报片能正确的重装成原来的数据报）	标志	3 （最低位 MF=1 表示后面还有分片， MF=0 表示这是若干个数据报片的最后一个 中间位 DF=0 才允许分片）
片偏移	片偏移指出较长的分组在分片后，某片在原分组中的相对位置，都是 8 字节的偏移位置	生存时间	数据报在网络中的生存时间，指最多经过路由器的跳数
协议	8 （指出该数据报携带的数据是何种协议，以使得目的主机的 IP 层知道应将数据部分上交给哪个处理程序）如 ICMP=1 IGMP=2 TCP=6 EGP=8	首部校验和	这个部分只校验首部，不包括数据部分，计算方法：将首部划分为多个 16 位的部分，然后每个 16 位部分取反，然后计算和，再将和取反放到首

	IGP=9 UDP=17 Ipv6=41 OSPF=89		部校验和。接收方收到后按同样的方法划分，取反，求和，在取反，如果结果为零，则接收，否则就丢弃
源地址	32	目的地址	32

（2）一个 TCP 报文段分为首部和数据两部分。首部由固定部分和选项部分组成，固定部分是 20 字节。 TCP 首部的最大长度为 60 。首部固定部分字段：

字段名	字节（ Byte ）	字段名	字节（ Byte ）
源端口	2	目的端口	2
序号	4	确认号	4 ，是期望收到对方的下一个报文段的数据的第一个字节的序号
数据偏移	4bit 指出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远	保留	6bit
紧急比特		确认比特 ACK	只有当 ACK=1 时，确认号字段才有效
推送比特		复位比特	
同步比特		终止比特	
窗口	2	检验和	2 （包括首部和数据两部分，同时还要加 12 字节的伪首部进行校验和计算）
选项	长度可变（范围 1 ——40 ）		

TCP 的 12 字节伪首部：

源 IP 地址（ 4 ）	目的 IP 地址（ 4）	0 (1)	6(1) 代表这是 TCP， IP 协议中提到过	TCP 长度（ 2 ）

（3）用户数据报 UDP 由首部和数据部分组成。首部只有 8 个字节，由 4 个字段组成，每个字段都是两个字节。

字段名	字节	字段名	字节
源端口	2	目的端口	2
长度	2	检验和	2（检验首部和数据，加 12 字节的伪首部）

UDP 的 12 字节伪首部：

源 IP 地址（4）	目的 IP 地址（4）	0 (1)	17(1) 代表这是 UDP， IP 协议中提到过	UDP 长度（2）

27、面向连接和非面向连接的服务的特点是什么？

答：面向连接的服务，通信双方在进行通信之前，要先在双方建立起一个完整的可以彼此沟通的通道，在通信过程中，整个连接的情况一直可以被实时地监控和管理。

非面向连接的服务，不需要预先建立一个联络两个通信节点的连接，需要通信的时候，发送节点就可以往网络上发送信息，让信息自主地在网络上去传，一般在传输的过程中不再加以监控。

28、以太网帧的格式

答：

目的地址	源地址	类型	数据	FCS

29、 TCP 的三次握手过程？为什么会采用三次握手，若采用二次握手可以吗？

答：建立连接的过程是利用客户服务器模式，假设主机 A 为客户端，主机 B 为服务器端。

（1） TCP 的三次握手过程：主机 A 向 B 发送连接请求；主机 B 对收到的主机 A 的报文段进行确认；主机 A 再次对主机 B 的确认进行确认。

（2）采用三次握手是为了防止失效的连接请求报文段突然又传送到主机 B，因而产生错误。失效的连接请求报文段是指：主机 A 发出的连接请求没有收到主机 B 的确认，于是经过一段时间后，主机 A 又重新向主机 B 发送连接请求，且建立成功，顺序完成数据传输。考虑这样一种特殊情况，主机 A 第一次发送的连接请求并没有丢失，而是因为网络节点导致延迟达到主机 B，主机 B 以为是主机 A 又发起的新连接，于是主机 B 同意连接，并向主机 A 发回确认，但是此时主机 A 根本不会理会，主机 B 就一直在等待主机 A 发送数据，导致主机 B 的资源浪费。

（3）采用两次握手不行，原因就是上面说的实效的连接请求的特殊情况。

30、电路交换、报文交换分组交换的比较？

答：电路交换：公共电话网（ PSTN 网）和移动网（包括 GSM 和 CDMA 网） 采用的都是电路交换技术，它的基本特点是采用面向连接的方式，在双方进行通信之前，需要为通信双方分配一条具有固定宽带的通信电路，通信双方在通信过程中 一直占用所分配的资源，直到通信结束，并且在电路的建立和释放过程中都需要利用相关的信令协议。这种方式的优点是在通信过程中可以保证为用户提供足够的带 宽，并且实时性强，时延小，交换设备成本低，但同时带来的缺点是网络带宽利用率不高，一旦电路被建立不管通信双方是否处于通话状态分配的电路一直被占用。**连接建立——数据传输——释放链接**

报 文交换：报文交换和分组交换类似，也采用存储转发机制，但报文交换是以报文作为传送单元，由于报文长度差异很大，长报文可能导致很大的时延，并且对每个节 点来说缓冲区的分配也比较困难，为了满足各种长度报文的需要并且达到高效的目的，节点需要分配不同大小的缓冲区，否则就有可能造成数据传送的失败。在实际 应用中报文交换主要用于传输报文较短，实时性要求较低的通信业务，如公用电报网，报文交换比分组交换出现的要早一些，分组交换是在报文交换的基础上，将报 文分割成分组进行传输，在传输时延和传输效率上进行了平衡。另外一个缺点是出错时，整个报文都将重传。

分 组交换：电路交换技术主要适用于传送话音相关的业务，这种网络交换方式对于数据业务而言，有着很大的局限性。首先是数据通信具有较强的突发性，峰值比特率 和平均比特率相差较大，如果采用电路交换技术，若按峰值比特率分配电路带宽会造成资源的极大浪费，如果按平均比特率分配带宽，则会造成数据的大量丢失，其 次是和语音业务比较，数据业务对时延没有严格的要求，但是需要进行无差错的传输，而语音信号可以有一定程序的失真但实时性要高。分组交换技术就是针对数据 通信业务的特点而提出的一种交换方式，它的基本特点是面向无连接而采用存储转发的方式，将需要传送的数据按照一定长度分割成许多小段数据，并在数据之前增 加相应的用于对数据进行选路和校验等功能的头部字段，作为数据传送的基本单元，即分组。采用分组交换技术，在通信之前不需要建立连接，每个节点首先将前一 节点送来的分组收下并保存在缓冲区中，然后根据分组头部中的地址信息选择适当的链路将其发送至下一个节点，这样在通信过程中可以根据用户的要求和网络的能 力来动态分配带宽。分组交换比电路交换的电路利用率高，但时延较大。分组转发的带来的问题：带来排队时延以及增加头部带来的开销。

31 、电信网络分类

电信网络

电路交换网络

分组交换网络

FDM

TDM

虚电路网络
数据报网络

32 、网络按地域范围分类？
答：局域网、城域网、广域网。

33 、网络按使用者分类为：公共网和专用网。

34 、网络的拓扑结构主要有：星形、总线型、环形以及树型、全连接、不规则网状。

星形　　树型

总线型　　环形

35 、计算机网络体系结构？
答：实际是分层加每层对应的协议集合。协议包括三个组成部分：
语法：数据与控制信息结构或格式；
语义：需要发出何种控制信息，完成何种动作以及做出何种响应；
时序（同步）：事件实现顺序的详细说明。

36 、双绞线的线对？
答： 1-2 、 7-8 、 3-6 、 4-5 白蓝 - 蓝、白橙 - 橙、白绿 - 绿、白棕 - 棕

37 、数据链路层协议可能提供的服务？
答：成帧、链路访问、透明传输、可靠交付、流量控制、差错检测、差错纠正、半双工和全双工。最重要的是帧定界（成帧）、透明传输以及差错检测。

38 、帧定界？
答：帧定界就是确定帧的界限，其方法有：字节计数法、字符填充法、零比特填充法。

39 、透明传输？
答：即应能传输任何的数据，在帧定界中用到的标记帧起点和结束的字符也应该能正确的被传输。

40 、差错检测？

答：循环冗余检验 CRC ，计算出的结果叫做帧检验序列 FCS 。循环冗余检验序列 CRC 差错检测技术只能做到无差错接受，即凡是接收端数据链路层接受的帧，我们都能以非常接近于 1 的概率认为这些帧在传输过程中没有产生差错，但是要做到可靠传输（即发送什么就收到什么），也就是说，传输到接收端的帧无差错、无丢失、无重复，同时还按发送的顺序接收，这时就必须再加上确认和重传机制。

41 、实现可靠传输的协议？

（ 1 ）停止等待协议：每发送完一帧就停止发送，直到收到接收到发送回来的确认在发送下一帧，如果没有收到接收端的确认，则通过设定的定时器超时了重传上一帧。其存在的三种可能：

重 传可能会导致接收端收到相同的帧，这时候根据序号来判定，如果收到的帧的序号之前已经被接收到了，则新接收到的帧被丢弃。因为可能会出现接收端不能在一次 情况就能正确接收，因此帧需要在发送端备份一份，直到被确认后才丢弃，因为该协议一次只能发送一帧，因此发送端的缓存区不需要太大。

（ 2 ）连续 ARQ 协议：发送窗口大于 1 ，接收窗口等于 1 ，因此发送窗口已经发送到了序号为 5 的帧，但是接收端接收到序号为 3 的帧出现错误时，那 3 号以后的帧都需要重传，因此出现错误的情况可能会导致重传多个帧，同时为了能够在出错时重传，因此发送出来还没有经过确认的帧都需要在发送端全缓区进行保存，这种情况需要的缓冲区比停止等待协议需要的更大。但采用 n 比特来表示编号时，则发送窗口的的大小为 时，该协议才能正确工作。若用 n 比特编号时，则发送窗口的大小 $WT<=2^n-1$。

（ 3 ）选择重传 ARQ 协议：发送窗口和接收窗口都大于 1 ，这种情况可能减少重传帧的数量，若用 n 比特编号时，则接收窗口的大小为 $\boldsymbol{WR \leq 2^n/2}$ 。

42 、 PPP 协议工作过程？

答：用户拨号接入 ISP ， ISP 的调制解调器对拨号做出确认，并建立一条物理链路，用户向 ISP 的路由器发送一系列的 LCP 分组，这是为 PPP 选择一些参数，然后配置网络层， NCP 为新接入的 PC 分配一个临时的 IP 地址，这样用户 PC 就成为因特网上的主机，通信结束后， NCP 释放网络层连接收回 IP 地址，然后， LCP 释放数据链路层连接，最后释放物理层的连接。

43 、数据链路层互联设备

答：（ 1 ）网桥：互连两个采用不同数据链路层协议，不同传输介质与不同传输速率的网络，网桥互连的网络在数据链路层以上采用相同的协议。

（ 2 ）交换机在数据链路层上实现互连的存储转发设备。交换机按每个包中的 MAC 地址相对简单地决策信息转发，交换机对应硬件设备，网桥对应软件。

44 、局域网的关键技术？

答：拓扑结构（星形，总线型，环形，树型），介质访问方式（ CSMA/CD ， Token-passing ），信号传输形式（基带、宽带）。

45 、网络接口卡（网卡）的功能？

答：（ 1 ）进行串行 / 并行转换。

（ 2 ）对数据进行缓存。

（ 3 ）在计算机的操作系统安装设备驱动程序。

（ 4 ）实现以太网协议。

46 、 CSMA/CD ？

答：是指载波监听多点接入 / 碰撞检测

（ 1 ）多点接入是指多台计算机以多点接入的方式连接在一条总线上

（ 2 ）载波监听是指每一个站在发送数据之前首先要检查一下总线上是否已经有其他计算机在发送数据，如果有，则暂时不要发送，避免碰撞

（ 3 ）实际在总线上并没有什么载波，实际是采用电子技术检测总线上是否有其他计算机发送的数据信号

（ 4 ）碰撞检测就是计算机边发送数据边检测信道上的信号电压大小，当发生了碰撞即产生了冲突，碰撞检测也叫做“冲突检测”

（ 5 ）当发生了碰撞时，总线上传输的信号就产生了失真，无法恢复出有用的信息，因此为了不浪费网络资源，一旦检测到碰撞发生时，就停止数据发送。然后再等待一段随机时间后在发送。

（ 6 ）强化碰撞，当检测到碰撞后，不仅立即停止发送数据外，还要人为的发送一些干扰信息，让其他站也知道此时碰撞发生了。

（ 7 ）由于信号在总线上的传输也是需要一定的时间的，所以当一个站检测到总线是空闲的时候，也可能并非是真正的空闲，因为会存在其他站发送了数据，只是还没有传送到该站能检测的范围内。这种情况下，发送数据最终也会导致碰撞发生。

（ 8 ）工作原理

（ 81 ）发送前先监听信道是否空闲，若空闲则立即发送；

（ 82 ）如果信道忙，则继续监听，一旦空闲就立即发送；

（ 83 ）在发送过程中，仍需继续监听。若监听到冲突，则立即停止发送数据，然后发送一串干扰信号（ Jam ）；

（ 84 ）发送 Jam 信号的目的是强化冲突，以便使所有的站点都能检测到发生了冲突。

等待一段随机时间（称为退避）以后，再重新尝试。

总结为四句话：发前先听，空闲即发送，边发边听，冲突时退避。

47 、以太网 MAC 帧格式？

答：

目的地址（ 6 字节）	源地址（ 6 字节）	类型（ 2 字节）	数据（ 46 —— 1500 字节）	FCS （ 4 字节）

48 、虚拟局域网 VLAN ？

答：（ 1 ） VLAN 只是局域网提供给用户的一种服务，而并不是一种新的局域网络。 VLAN 限制了接收广播消息的工作站数，使得网络不会因传播过多的广播信息（即广播风暴）而引起性能恶化。

（ 2 ）划分 VLAN 的方法：基于端口；基于 MAC 地址；基于 IP 地址。

（ 3 ） VLAN 的帧格式

目的地址（ 6 字节）	源地址（6 字节）	VLAN 标记（表明该站是属于哪个 VLAN 的）	类型（ 2 字节）	数据（ 46 —— 1500 字节）	FCS （ 4 字节）

49 、无线局域网的 MAC 层？

答：（ 1 ）隐藏站问题，暴露站问题

（ 2 ） CSMA/CA ：是改进的 CSMA/CD ，增加的功能是碰撞避免，实际就是在发送数据之前对信道进行预约。

50 、 NAT ？

答：（ 1 ）网络地址转换，是一种将私有地址转换为合法 IP 地址的转换技术，这种技术可以解决现在 IP 地址不够的问题。

（ 2 ） NAT 的实现方式：静态转换；动态转换；端口多路复用（即 内部 IP+ 端口号——外部 IP+ 端口号，这种方式改变外出数据包的源端口并进行端口转换，内部网络的所有主机都可共享一个合法外部 IP 地址实现对 Internet 的访问，从而节约 IP 资源，同时隐藏网络内部的所有主机，有效避免来自 Internet 的攻击）。

（ 3 ）缺点：由于需要将 IP 包头中的 IP 地址进行转换，因此不能进行加密操作。

51 、私有（保留）地址？

答： A 类： 10.0.0 .0 —— 10.255.255.255

B 类： 172.16.0.0 —— 172.31.255.255

C 类： 192.168.0.0 —— 192.168.255.255

52 、交换和路由的区别是什么？ VLAN 有什么特点？

答：交换是指转发和过滤帧，是交换机的工作，它在 OSI 参考模型的第二层，而路由是指网络线路当中非直连的链路，它是路由器的工作，在 OSI 参考模型的第三层。交换和路由的区别很多，首先，交换是不需要 IP 地址的，而路由需要，因为 IP 就是第三层的协议，第二层需要的是 MAC 地址，再有，第二层的技术和第三层的不一样，第二层可以做 VLAN ，端口捆绑等，第三层可以做 NAT ， ACL ， QoS 等。

VLAN 是虚拟局域网的英文缩写，它是一个纯二层的技术，它的特点有三：控制广播，安全，灵活性和可扩张性。

53 、 SNMP ？

答：简单网络管理协议的英文缩写。

54 、 TTL 是什么？作用是什么？哪些工具会用到它（ ping traceroute ifconfig netstat ）？

答： TTL 是指生存时间，简单来说，它表示了数据包在网络中的时间，经过一个路由器后 TTL 就减一，这样 TTL 最终会减为 0 ，当 TTL 为 0 时，则将数据包丢弃，这样也就是因为两个路由器之间可能形成环，如果没有 TTL 的限制，则数据包将会在这个环上一直死转，由于有了 TTL ，最终 TTL 为 0 后，则将数据包丢弃。 ping 发送数据包里面有 TTL ，但是并非是必须的，即是没有 TTL 也是能正常工作的， traceroute 正是因为有了 TTL 才能正常工作， ifconfig 是用来配置网卡信息的，不需要 TTL ， netstat 是用来显示路由表的，也是不需要 TTL 的。

55 、路由表是做什么用的？在 Linux 环境中怎么配置一条默认路由？

答： 路由表是用来决定如何将一个数据包从一个子网传送到另一个子网的，换句话说就是用来决定从一个网卡接收到的包应该送到哪一个网卡上去。路由表的每一行至少 有目标网络号、子网掩码、到这个子网应该使用的网卡这三条信息。当路由器从一个网卡接收到一个包时，它扫描路由表的每一行，用里面的子网掩码与数据包中的 目标 IP 地址做逻辑与运算（ & ）找出目标网络号。如果得出的结果网络号与这一行的网络号相同，就将这条路由表六下来作为备用路由。如果已经有备用路由了，就载这两条路由里将网络号最长的留下来，另一条丢掉（**这是用无分类编址 CIDR 的情况才是匹配网络号最长的，其他的情况是找到第一条匹配的行时就可以进行转发了**）。如此接着扫描下一行直到结束。如果扫描结束仍没有找到任何路由，就用默认路由。确定路由后，直接将数据包送到对应的网卡上去。在具体的实现中，路由表可能包含更多的信息为选路由算法的细节所用。

在 Linux 上可以用“ route add default gw< 默认路由器 IP> ”命令配置一条默认路由。

56 、每个路由器在寻找路由时需要知道哪 5 部分信息？

答：目的地址：报文发送的目的地址

邻站的确定：指明谁直接连接到路由器的接口上

路由的发现：发现邻站知道哪些网络

选择路由：通过从邻站学习到的信息，提供最优的到达目的地的路径

保持路由信息：路由器保存一张路由表，它存储所知道的所有路由信息。

57 、 EGP ， IGP ？

答：（ 1 ） IGP ：内部网关协议，即在一个自治系统内部使用的路由选择协议，如 RIP 和 OSPF 。

（ 11 ） RIP 是一种分布式的基于距离向量的路由选择协议，要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的距离向量。距离即是跳数，路由器与直接相连的网络跳数为 1 ，以后每经过一个路由器跳数加 1 。 RIP 允许一条路径最多包含 15 个路由器，因此当距离为 16 时认为不可达，这因为如此限制了网络的规模，说明 RIP 只能工作在规模较小的网络中。 **RIP 的三个要点：仅和相邻路由器交换信息；交换的信息是当前路由器知道的全部信息，即路由表；按固定的时间间隔交换路由信息，如 30 秒。 RIP 协议使用运输层的用户数据报 UDP 进行传送，因此 RIP 协议的位置位于应用层，但是转发 IP 数据报的过程是在网络层完成的。 RIP 是好消息传播的快，坏消息传播的慢。**

（ 12 ） OSPF ：最短路径优先，三个要点：采用洪泛法向本自治系统的路由器发送信息；发送的信息就是与本路由器相邻的所有路由器的链路状态，但这只是路由器所知道的部分信息；只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送此信息。 OSPF 直接使用 IP 数据包传送，因此 OSPF 位于网络层。

EGP ：外部网关协议，若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议将路由选择信息传递到另一个自治系统中，如 EGP 。

58 、自适应网卡只有红灯闪烁，绿灯不亮，这种情况正常吗？

答：正常。自适应网卡红灯代表连通 / 工作，即连通时红灯长亮，传输数据时闪烁，绿灯代表全双工，即全双工状态是亮，半双工状态灭。如果一个半双工的网络设备（如 HUB ）和自适应网络相连，由于这张网卡是自适应网卡，它就会工作在半双工状态，所以绿灯不亮也属于正常情况。

补充：网卡红绿灯是网卡工作的指示灯，红灯亮表示正在发送或接收数据，绿灯亮则表示网络连接正常。因此正常情况下应该是绿灯长亮，因为绿灯长亮才代表网络是通的。而有数据传输时，红灯就会闪烁。

59 、两台笔记本电脑连起来后 ping 不同，你觉得可能存在哪些问题？

答：（ 1 ）首先考虑是否是网络的问题

（ 2 ）局域网设置问题，电脑互联是要设置的。看是否安装了必要的网络协议，最重要的是 IP 地址是否设置正确。

（ 3 ）网卡驱动未安装正确

（ 4 ）防火墙设置有问题

（ 5 ）是否有什么软件阻止了 ping 包

60 、与 IP 协议配套的其他协议？

答： ARP ：地址解析协议　　RARP ：逆地址解析协议

ICMP ：因特网控制报文协议　　IGMP ：因特网组管理协议

其关系为：

61 、 IP 地址分类？

答： IPv4 地址共有 32bit

	网络号	网络范围	主机号
A 类	8bit　第一位固定为 0	0 —— 127	24bit
B 类	16bit　前两位固定为 10	128.0 —— 191.255	16bit
C 类	24bit　前三位固定为 110	192.0.0 —— 223.255.255	8bit
D 类	前四位固定为 1110 ，后面为多播地址　**所以 D 类地址为多播地址**		
E 类	前五位固定为 11110 ，后面保留为今后所用		

一般全 0 或全 1 的地址不使用，有特殊意思，主机地址为全 1 时为广播地址，全 0 时表示网络地址。同时 127.0.0.1 表示回路， ping 该 IP 地址可以测试本机的 TCP/IP 协议安装是否成功。

62 、 RARP ？

答：逆地址解析协议，作用是完成硬件地址到 IP 地址的映射，主要用于无盘工作站，因为给无盘工作站配置的 IP 地址不能保存。工作流程：在网络中配置一台 RARP 服务器，里面保存着 IP 地址和 MAC 地址的映射关系，当无盘工作站启动后，就封装一个 RARP 数据包，里面有其 MAC 地址，然后广播到网络上去，当服务器收到请求包后，就查找对应

的 MAC 地址的 IP 地址装入响应报文中发回给请求者。因为需要广播请求报文，因此 RARP 只能用于具有广播能力的网络。

63 、划分子网？

答：从大的方面来看，跟只有网络号和主机号的分类方式类似，这是由分配到网络号的网络内部自己在进行分配，是从主机号部分借用位来形成子网，涉及到子网时，就要有子网掩码，一个涉及到了子网的 IP 地址的网络号等于该 IP 地址与子网掩码的与（ & ）运算的结果。

64 、 IPv6 ？

答：采用 128bit ，首部固定部分为 40 字节。

65 、运输层协议与网络层协议的区别？

答：网络层协议负责的是提供主机间的逻辑通信

运输层协议负责的是提供进程间的逻辑通信

66 、运输层的协议？

答： TCP ，传输单位称为： TCP 报文段

UDP ，传输单位称为：用户数据报

其端口的作用是识别那个应用程序在使用该协议。

67 、接入网用的是什么接口？

答：一般采用 E1 ， V.24 ， V.35 ，等接口。

68 、直接链接两个信令点的一组链路称作什么？

答： PPP 点到点连接。