交换机计费方式与采用的计费系统、业务的类型以及 入网的方式有关，主要有如下三种：
1 CAMA 计费系统
CAMA 计 费 系 统 即 Centralized Automatic Message Accounting System－集中式自动通话记帐系统的简称，又称为详细帐单 （Detail billing）方式。
2 LAMA 计费系统
LAMA 计费系统即 Local Automatic Message Accounting System－本地自动 通话记帐系统的简称，也叫市话计费方式。
3 PAMA 计费系统
在国内交换机中，长途交换局一般采用 CAMA 方式，市话局采用 LAMA 方式，而长市 合一局二者均需采用。

中继器、网卡：工作在物理层；
网桥：数据链路层；
路由器：网络层

运输层的端口号共分为以下两大类：
1，服务器端使用的端口号 ： 这里面又分为两类。a，熟知端口号（也叫系统端口号），数值为 0~1023.IANA 把这些端口号指派给了 TCP/IP 最重要的一些应用程序，让所有的用户都知道。如 FTP：21，TELNET：23，HTTP：80，DNS：53 等。b，登记端口号，数值为 1024~49151.这类端口号是为没有熟知端口号的应用程序使用的，使用这类端口号必须在 IANA 按照规定的手续登记，以防止重复。
2，客户端使用的端口号：数值为 49152~65535.由于这类端口号仅在客户进程运行时才动态选择，因此又叫做短暂端口号。这类端口号是留给客户进程选择暂时使用。当服务器进程收到客户进程的报文时，就知道了客户进程所使用的端口号，因而可以把数据发送给客户进程。通信结束后，刚才已使用的客户端口号就不复存在。这个端口号就可以供其他客户进程以后使用。
根据以上说明 ，1~49151 端口号，都需要 root 权限才能打开。故 AD 错误。而 C 中 8080 端口号相当于是使用 HTTP 协议的后门，他并不是特定为 http 服务的，只是用于 www 代理服务，而由于 8080 方便与 http（80 端口号）配套记忆，故常优先分配给 http 使用。C 错误。
一共有 65535 个端口可用。小于 1023（包括 1023）的端口只有 root 身份才能启动。这些端口为预留端口，被分配给一些常见的重要服务（如：HTTP、FTP、SSH 等）。
大于 1024 的端口作为随机分配之用。

HTTP 的 cookie 是明文传送的，HTTPS 的 cooike 是密文传送的。

路由算法修改路由表的基本目的是将最好路由信息添加到路由表中，路由的 好坏是由路由算法根据自己获得的路由信息计算出来的。对于每一条路由， 路由算法产生一种权值来表示路由的好坏。通常情况下，这种权值越小，该路径越好。 路由权的计算可能基于路径某单一特性计算，也可能基于路径多种属性进行计算。

ICMP 是（Internet Control Message Protocol）Internet 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 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。
TCP/IP 详解卷一中是这样解释的：“ping”这个名字源于声纳定位操作 Ping 程序由 Mike Muuss 编写，目的是为了测试另一台主机是否可达。该程序发送一份 ICMP 回显请求报文给主机，并等待返回 ICMP 回显应答。
ICMP 是 IP 层的一个组成部分，它传递差错报文以及其它需要注意的信息。ICMP 报文通常被 IP 层或更高层协议使用
ICMP Internet Control Message Protocol 网间控制报文协议
TCP/IP 协议族中的一种协议，位于 IP 层，用于传输网络中的控制信息。ICMP 允许出错消息的生成、检测分组和与 IP 相关的信息邮件。

理层： RJ45 、 CLOCK 、 IEEE802.3 （中继器，集线器，网关） -
数据链路： PPP 、 FR 、 HDLC 、 VLAN 、 MAC （网桥，交换机） -

网络层： IP 、 ICMP 、 ARP 、 RARP 、 OSPF 、 IPX 、 RIP 、 IGRP 、 （路由器） -
传输层： TCP 、 UDP 、 SPX -
会话层： NFS 、 SQL 、 NETBIOS 、 RPC -
表示层： JPEG 、 MPEG 、 ASII -
应用层： FTP 、 DNS 、 Telnet 、 SMTP 、 HTTP 、 WWW 、 NFS

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。

分 3 个子网，网络位必须向地址位借 2 位 也就是说 子网掩码为 255.255.255.192.0 这样可以划分出 4 个子网！每个子网能容纳 62 台主机！ 经过验算得出
255.255.255. 192 选 D 选项
可以从容纳主机数量的角度出发。主机号 n 位 2 的 n 次方-2>55，n 至少为 6，又要划分 3 个机房，至少要借两位。满足以上两个条件，借位只能为 2.C 类地址，子网掩码默认为 24 位，既 255.255.255.0,借两位以后，变成 255,255,255,192
C 类网址：24 位网络 ID + X 位子网 ID + （8-X）位主机地址
只有 C 满足要求
子网掩码为 255.255.255.192
192 为 11000000，子网 ID 为 2 位，6 位为主机地址。子网数为 2 的平方为 4 个（>3），每个子网的主机号为 2^6-2 = 62 个(>55)。

ICMP 是（Internet Control Message Protocol）Internet 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 是否可用等网络本身的消息
在 IPv4 协议中最常用的 ICMP 消息类型有以下几种:
• 回显应答(类型 0)和回显请求(类型 8):这是 Ping 程序发送的信息。
•目标不可达(类型 3)
•源抑制(类型 4):这是一种用于通知发送者路由器或者主机出现阻塞现象的 ICMP 消息，发送者需要降低发送速度。
•重定向(类型 5):这个消息用来向可以访问两台路由器的主机说“请使用另一台路由器”。
•路由器信息应答(类型 9)和路由器信息请求(类型 10)
•超时(类型 11):这个消息有两种用途。第一，当超过 IP 生存期时向发送系统发出错误信息。第二，如果分段的 IP 数据报没有在某种时限内重新组合，这个消息将通知发送系统。

RARP 协议：根据 MAC 地址查找对应的 IP 地址。NAT 协议把公网的 IP 地址转换为私网的 IP 地址。ICMP 协议用于控制数据报传送中的差错情况。DHCP 协议用于集中管理网络中的 IP 地址分配。

A time_wait 需要等待 2msl，防止 ack 丢失
B shutdown 可以使 TCP 半双工，但是如果之前调用了 close，则直接关闭了 socket
C 收到了 ack 之后的状态，是只能接受不能发送
D 会有很多意外情况，例如 rst
发表于 2015-08-12 12:02:19

TIME_WAIT 状态下发送的 ACK 丢失，服务器端的 LAST_ACK 时刻设定的重传定时器超时，发送重传的 FIN，很不幸，这个 FIN 也丢失，主动关闭方在 TIME_WAIT 状态等待 2MSL 没收到任何报文段，进入 CLOSED 状态，当此时被动关闭方并没有收到最后的 ACK。所以即使要主动关闭方在 TIME_WAIT 状态下停留 2MSL，也不一定表示四次握手关闭就一定正常完成

NAT 定义

NAT（Network Address Translation，网络地址转换）是 1994 年提出的。当在专用网内部的一些主机本来已经分配到了本地 IP 地址（即仅在本专用网内使用的专用地址），但现在又想和因特网上的主机通信（并不需要加密）时，可使用 NAT 方法。

这种方法需要在专用网连接到因特网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 NAT 路由器，它至少有一个有效的外部全球 IP 地址。这样，所有使用本地地址的主机在和外界通信时，都要在 NAT 路由器上将其本地地址转换成全球 IP 地址，才能和因特网连接。

NAT 功能

NAT 不仅能解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

1.宽带分享：这是 NAT 主机的最大功能。

2.安全防护：NAT 之内的 PC 联机到 Internet 上面时，他所显示的 IP 是 NAT 主机的公共 IP，所以 Client 端的 PC 当然就具有一定程度的安全了，外界在进行 portscan（端口扫描） 的时候，就侦测不到源 Client 端的 PC 。

NAT 实现方式

NAT 的实现方式有三种，即静态转换 Static Nat、动态转换 Dynamic Nat 和端口多路复用 OverLoad。

静态 转换是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备（如服务器）的访问。

动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的，所有被授权访问上 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时。可以采用动态转换的方式。

端口多路复用（ Port address Translation,PAT)是指改变外出数据包的源端口并进行端口转换，即端口地址转换（PAT，Port Address Translation).采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自 internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

NAT 配置

在配置 NAT(网络地址转换)之前，首先需要了解内部本地地址和内部全局地址的分配情况。根据不同的需求，执行以下不同的配置任务。

内部源地址 NAT 配置

内部源地址 NAPT 配置

重叠地址 NAT 配置

TCP 负载均衡

采用 NAT 时，在虚拟机中，不用做任何配置，只要宿主机器访问网络即可。

MPLS(Multiprotocol Label Switching,多协议标记交换.) VPN

是在网络路由和交换设备上应用 MPLS 技术.采用路由隔离、地址隔离等多种手段提供了抗攻击和标记欺骗的手段，在 MPLS VPN 传递数据，只是标记了端点路由，对数据本身并不提供加密的防护手段。因此 MPLS VPN 的安全性一般。

IPSEC(Internet Protocol Security) VPN 是完全基于 INTERNET 构建的

IPSEC VPN 为了实现在 Internet 上安全的传递数据，采用了对称密钥、非对称密钥以及摘要算法等多种加密算法，通过身份认证、数据加密、数据完整性校验等多种方式保证接入的安全，保证的数据的私密性。

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。

直接路由是指路由器各网络接口所直连的网络之间进行通信所使用的路由。直接路由是在配置完路由器网络接口的 IP 地址后自动生成的，因此，如果没有对这些接口进行特殊的限制，这些接口所直连的网络之间就可以直接通信。

缺省路由是一种特殊的路由，可以通过静态路由配置，某些动态路由协议也可以生成缺省路由，如 OSPF 和 IS-IS。在小型互连网中，使用缺省路由可以减轻路由器对路由表的维护工作量，从而降低内存和 CPU 的使用率。

动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。

所以静态路由和缺省路由由网管手动配置。
所以答案选 A 和 C

Internet 分组交换/顺序分组交换 IPX/SPX(Internetwork Packet Exchange/Sequences Packet Exchange)是 Novell 公司的通信协议集。与 NetBEUI 形成鲜明区别的是 IPX/SPX 比较庞大，在复杂环境下具有很强的适应性。这是因为 IPX/SPX 在设计一开始就考虑了网段的问题，因此它具有强大的路由功能，适合于大型网络使用。当用户端接入 NetWare 服务器时，IPX/SPX 及其兼容协议是最好的选择。但在非 Novell 网络环境中，一般不使用 IPX/SPX。

MAC 地址，or 硬件地址/物理地址，长度是 48 比特（6 字节）(每个字节之间的分隔符并没有严格要求 可以说冒号 or 减号)，由 16 进制的数字组成。
分为前 24 位和后 24 位：
前 24 位叫做组织唯一标志符（Organizationally Unique Identifier，即 OUI），是由 IEEE 的注册管理机构给不同厂家分配的代码，区分了不同的厂家。
后 24 位是由厂家自己分配的，称为扩展标识符。同一个厂家生产的网卡中 MAC 地址后 24 位是不同的。

TCP/IP 协议，或称为 TCP/IP 协议栈，或互联网协议系列。
TCP/IP 协议栈（按 TCP/IP 参考模型划分），TCP/IP 分为 4 层，不同于 OSI，他将 OSI 中的会话层、表示层规划到应用层。
应用层 FTP SMTP HTTP ...
传输层 TCP UDP
IP 网络层 IP ICMP IGMP
网络接口层 ARP RARP 以太网令牌环 FDDI ...
包含了一系列构成互联网基础的网络协议。

HTTPS 在传输数据之前需要客户端（浏览器）与服务端（网站）之间进行一次握手，在握手过程中将确立双方加密传输数据的密码信息。TLS/SSL 协议不仅仅是一套加密传输的协议，更是一件经过艺术家精心设计的艺术品，TLS/SSL 中使用了非对称加密，对称加密以及 HASH 算法。握手过程的简单描述如下：
1.浏览器将自己支持的一套加密规则发送给网站。
2.网站从中选出一组加密算法与 HASH 算法，并将自己的身份信息以证书的形式发回给浏览器。证书里面包含了网站地址，加密公钥，以及证书的颁发机构等信息。
3.获得网站证书之后浏览器要做以下工作：
a) 验证证书的合法性（颁发证书的机构是否合法，证书中包含的网站地址是否与正在访问的地址一致等），如果证书受信任，则浏览器栏里面会显示一个小锁头，否则会给出证书不受信的提示。
b) 如果证书受信任，或者是用户接受了不受信的证书，浏览器会生成一串随机数的密码，并用证书中提供的公钥加密。
c) 使用约定好的 HASH 计算握手消息，并使用生成的随机数对消息进行加密，最后将之前生成的所有信息发送给网站。
4.网站接收浏览器发来的数据之后要做以下的操作：
a) 使用自己的私钥将信息解密取出密码，使用密码解密浏览器发来的握手消息，并验证 HASH 是否与浏览器发来的一致。
b) 使用密码加密一段握手消息，发送给浏览器。
5.浏览器解密并计算握手消息的 HASH，如果与服务端发来的 HASH 一致，此时握手过程结束，之后所有的通信数据将由之前浏览器生成的随机密码并利用对称加密算法进行加密。
这里浏览器与网站互相发送加密的握手消息并验证，目的是为了保证双方都获得了一致的密码，并且可以正常的加密解密数据，为后续真正数据的传输做一次测试。另外，HTTPS 一般使用的加密与 HASH 算法如下：
非对称加密算法：RSA，DSA/DSS
对称加密算法：AES，RC4，3DES
HASH 算法：MD5，SHA1，SHA256

答案： 服务器端建立 TCP 连接的状态
思路：
1. 建立 TCP 连接需要经过三次握手，如下
2. 首先服务器端处于 LISTEN 状态，等待客户端的连接
3. 客户端向服务器端发送 SYN 报文，此时客户端处于 SYN_SENT 状态
4. 服务器端接收到 SYN 报文后，向客户端发送 ACK 报文，处于 SYN_RECEIVED 状态，等待接收客户端的 ACK 报文
5. 当服务器端收到客户端的 ACK 报文后，建立 TCP 连接，此时处于 ESTABLISHED 状态

tcpdump 是简单可靠网络监控的实用工具
top 显示活动进程方面的情况
netstat 显示网络有关的信息，比如套接口使用情况、路由、接口、协议（TCP 等）等
ifconfig 是查看活动的网卡信息

1 http 的 keepalive 受限于 idle 时间，据 google 的统计(chrome 浏览器),尽管 chrome 开启了 http 的 keepalive(chrome 是 4 分钟)，可是依然有 35%的请求是重新发起一条连接。而三次握手会造成一个 RTT 的延迟，因此 TFO 的目标就是去除 这个延迟，在三次握手期间也能交换数据。
2 RFC793 允许在 syn 数据包中带数据，可是它要求这些数据必须当 3 次握手之后才能给应用程序，这样子做主要是两个原因，syn 带数据可能会引起 2 个问 题。第一个是有可能会有前一个连接的重复或者老的数据的连接(syn+data 的数据)，这个其实就是三次握手的必要性所决定的。第二个就是最重要的，也 就是安全方面的，为了防止攻击。
3 而在 TFO 中是这样解决上面两个问题的，第一个问题，TFO 选择接受重复的 syn,它的观点就是有些应用是能够容忍重复的 syn+data 的(幂等的操 作)，也就是交给应用程序自己去判断需不需要打开 TFO。比如 http 的 query 操作(它是幂等的).可是比如 post 这种类型的，就不能使用 TFO， 因为它有可能会改变 server 的内容. 因此 TFO 默认是关闭的，内核会提供一个接口为当前的 tcp 连接打开 TFO。为了解决第二个问题，TFO 会有一个 Fast Open Cookie(这个是 TFO 最核心的一个东西),其实也就是一个 tag。
4 启用 TFO 的 tcp 连接也很简单，就是首先 client 会在一个请求中(非 tfo 的)，请求一个 Fast Open Cookie(放到 tcp option 中),然后在下次的三次握手中使用这个 cookie(这个请求就会在 3 次握手的时候交换数据).
客户端通过 TCP 连接到服务器时，可以在 SYN 报文携带数据，这将提升 TCP 的效率(4%-41%)[5]。前提是在这个 SYN 报文中，有代表客户端的在之前的 TCP 连接中服务器产生的 cookie 字段。在客户端和服务器第一次的 TCP 连接创建过程中，是通常的三次握手过程，但是服务器会产生 cookie 作为后续 TCP 连接的认证信息，这就避免了恶意攻击。对于客户端用户程序来说，可直接使用 sendto 等带有对端地址的系统调用发送数据，如果是第一次连接（或者 cookie 过期），则退化到正常三次握手过程，如果是非第一次连接，则可以继续创建连接且能够直接将数据交付给应用层处理。

ip 数据包将在此虚电路(vc)上以直通（cut-through）方式而下，再经过路由器，从而有效的解决了 ip 的路由器的瓶颈问题，并将 ip 包的转发速度提高到交换速度

IP over ATM 技术是为了解决或是弥补 IP 网的缺点而出现的，ATM 属于二层传递使用虚通路标识来传递信息，主要优点就是选择固定长度的信元作为传输单位有利于高速交换；支持不同速率的各种业务；面向连接保证了实时性和服务质量；使用光纤信道误码率低，无需差错检测和流量控制。
IP 是三层协议，是现在使用最广的协议，是一种无连接的。二者实现优势互补，以结局宽带应用问题，并最终实现基于 IP 的实时多媒体业务。主要优点就是提供告诉点对点的连接，大大提高 IP 网的宽带 ；提供优良的网络性能，完善、成熟的 QoS 保证。
ATM 是异步传输模式的缩略语，ATM 采用面向连接的交换方式，它以信元为单位。之所以称其为异步，是因为来自某一用户的、含有信息的信息元重复出现不是周期性的。

在网络上是根据 ip 地址区分，局域网连路层根据 mac 地址，在主机上，应用系统会为应用程序分配端口号

服务器：socket();//socket 要求必须绑定 socket；
bind();//绑定端口和 IP，这样我们才知道是那台主机；
listen();//监听，看有没有请求连接
accept();//接收请求
send()||rev();//接收和发送消息
客户端：socket();//socket 要求必须绑定 socket；
connect();//请求连接

TCP 建立连接 3 次握手,断开链接需要 4 次

我国对独立型 STP 设备要求其信令链路数不得小于 512
由于 IP 地址唯一确定，就看端口号有多少了，不同的端口号可以连接不同的服务端，端口号的长度为 16 为，2*16 次方，所以最多为 65535 个。

ADSL 是非对称数字用户线路（Asymmetric Digital Subscriber Line）的缩写，亦可称作非对称数字用户环路。ADSL 技术提供的上行和下行带宽不对称，因此称为非对称数字用户线路，是一种异步传输模式（ATM）。

智能网由业务交换点（SSP）、业务控制点（SCP）、信令转接点（STP）、智能外设（IP）、业务管理系统（SMS）和业务生成环境（SCE）等组成，智能网的总体结构如图所示。
业务交换点（SSP）具有呼叫处理功能和业务交换功能。呼叫处理功能接收用户呼叫；业务交换功能接收、识别智能业务呼叫，并向 SCP 报告，接收 SCP 发来的控制命令。SSP 一般以原有的数字程控交换机为基础，升级软件，增加必要的硬件以及 NO.7 信令网的接口。目前中国智能网采用的 SSP 一般内置 IP，SSP 通常包括业务交换功能（SSF）和呼叫控制功能（CCF），还可以含有一些可选功能，如专用资源功能（SRF）、业务控制功能（SCF）、业务数据功能（SDF）等。
业务控制点（SCP）是智能网的核心。它存储用户数据和智能网业务逻辑，主要功能是接收 SSP 送来的查询信息，并查询数据库，进行各种译码。它根据 SSP 送来的呼叫事件启动不同的业务逻辑，根据业务逻辑向相应的 SSP 发出呼叫控制指令，从而实现各种各样的智能呼叫。SCP 一般由大、中型计算机和大型实时高速数据库构成，要求具有高度的可靠性，双备份配置。若数据库作为独立节点设置，则称为业务数据点（SDP）。目前中国智能网采用的 SCP 一般内置 SDP，一个 SCP 含有业务控制功能（SCF）和业务数据功能（SDF）。
信令转接点（STP）实际上是 NO.7 信令网的组成部分。在智能网中，STP 双备份配置，用于沟通 SSP 与 SCP 之间的信令联系，其功能是转接 NO.7 信令。
智能外设（IP）是协助完成智能业务的特殊资源，通常具有各种语音功能，如语声合成、播放录音通知、进行语音识别等。IP 可以是一个独立的物理设备，也可以是 SSP 的一部分。它接受 SCP 的控制，执行 SCP 业务逻辑所指定的操作。IP 含有专用资源功能（SRF）。
业务管理系统（SMS）是一种计算机系统。具有业务逻辑管理、业务数据管理、用户数据管理，业务监测和业务量管理等功能。在 SCE 上创建的新业务逻辑由业务提供者输入到 SMS 中，SMS 再将其装入 SCP，就可在通信网上提供该项新业务。一个智能网一般仅配置一个 SMS。

集线器的英文称为“Hub”。“Hub”是“中心”的意思，集线器的主要功能是对接收到的信号进行再生整形放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。它工作于 OSI(开放系统互联参考模型)参考模型第一层，即“物理层”。集线器与网卡、网线等传输介质一样，属于局域网中的基础设备，采用 CSMA/CD（即带冲突检测的载波监听多路访问技术)介质访问控制机制。集线器每个接口简单的收发比特，收到 1 就转发 1，收到 0 就转发 0，不进行碰撞检测。
集线器（hub）属于纯硬件网络底层设备，基本上不具有类似于交换机的"智能记忆"能力和"学习"能力。它也不具备交换机所具有的 MAC 地址表，所以它发送数据时都是没有针对性的，而是采用广播方式发送。也就是说当它要向某节点发送数据时，不是直接把数据发送到目的节点，而是把数据包发送到与集线器相连的所有节点，如图所示，简单明了。

HUB 和交换机的区别是:以一个 10M 的 HUB 和一个 10M 的交换机为例,HUB 的每个端口带宽(正在使用)之和等于 10M. 而交换机是每个端口都是 10M.因而 HUB 的传输过程数据产生碰撞较多,用户越多,性能越差,而交换机就不存在这个问题.

集线器不管有多少个端口，所有端口都共享一条带宽，在同一时刻只能有两个端口传送数据，其他端口只能等待；只能工作在半双工模式下。交换机每个端口都有一条独占的带宽，当两个端口工作时并不影响其他端口的工作，交换机可以工作在半双工模式下也可以工作在全双工模式下。

A 类地址 8bit 网络号 + 24bit 主机号
B 类地址 16bit 网络号 + 16bit 主机号
C 类地址 24bit 网络号 + 8bit 主机号
D 类地址 多播地址
E 类地址 保留

要使 CSMA/CA 正常工作，我们必须要限制帧的长度。如果某次传输发生了碰撞，那么正在发送数据的站必须在发送该帧的最后一比特之前放弃此次传输，因为一旦整个帧都被发送出去，那么该站将不会保留帧的复本，同时也不会继续监视是否发生了碰撞。（当发生了碰撞时，数据帧如果全部发送出去，受到损伤的数据发送出去后将无法更正；如果当发生碰撞后，另外一个站中的数据到达本站，而此时帧尚未完全发送出去，那么就可以放弃传输，然后就可以再次发送完整的数据，这个过程是正确执行，我们所希望看到的效果）因此帧的传输时间 Trf 必须是最大传播时间 Tp 的两倍（刚好本站的数据传播到目的站后，目的站刚好传播数据，发生碰撞）。

304 未修改（表示客户机缓存的版本是最新的，客户机应该继续使用它。）
404 找不到改页面
302 暂时重定向 2 次请求
400 代表客户端发起的请求不符合服务器对请求的某些限制，或者请求本身存在一定的错误。

IPV4 下，两种基本的通信方式分别是 TCP 和 UDP，前者是面向连接的可靠的字节流服务，通信之前必须要先建立起 socket 连接，而后者是面向无连接的数据包服务，通信之前无需建立起任何连接，因而 B 选项是错误的。

1、当给 WEB 服务器接上网线的时候，它会自动发送一条 ARP 信息，使得接入网关能找的到它；
网关上会形成一条类似：2c 96 1e 3c 3e 9b - 192.168.1.123 的 MAC 地址到 IP 地址的映射记录。
2、当第一个用户使用域名访问 WEB 服务器的时候，首先要进行一次 DNS 查询
3、最后才是 http 协议

由于 TCP 基于连接的，为了在服务端和客户端之间传送 TCP 数据，必须先建立一个虚拟电路，也就是 TCP 连接，建立 TCP 连接的过程也就是我们熟悉的“三次握手”过程：首先，请求端（客户端）发送一个包含 SYN 标志的 TCP 报文，表示客户端欲发起通信连接；第二步，服务器在收到客户端的 SYN 报文后，将返回一个 SYN+ACK 的报文，表示客户端的请求被接受；第三步，客户端也返回一个确认报文 ACK 给服务器端，到此一个 TCP 连接完成。问题就出在 TCP 连接的三次握手中，假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的，这种情况下服务器端一般会重试（再次发送 SYN+ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒-2 分钟）；如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源，最终导致服务器端忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求，此时从正常客户的角度看来，服务器失去响应，这种情况我们称作：服务器端受到了 SYN Flooding 攻击。

TCP 协议原理：TCP 每发送一个报文段，就启动一个定时器，如果在定时器超时之后还没有收到 ACK 确认，就重传该报文。 如图所示，数据包由 A 的缓冲区发往 B，B 在收到数据包以后，回发一个 ACK 确认包给 A，之后 A 将该数据包从缓冲区释放。因此，该数据包会一直缓存在 A 的缓冲区，直到一个 ACK 确认为止。题目要求在 100s 内发送

100GB 数据，网络的传输速率至少是 1G/s，某个数据包 n 在 A 中缓存的时间就是数据包 n 从 A 到 B，再加上该数据包的 ACK 从 B 到 A 的时间：2*1500m/(2*108m/s)=1.5*10-2s，该段时间 A 中缓存的数据量至少是 1G/s*1.5*10-2s 约为 15M

表示层功能：数据的编码、翻译、压缩、解压缩、加密、解密，将数据翻译为相对应的编码格式，然后展现到应用程序中，包含 JPEG 、 ASCII 、 TIFF 、 GIF 、 PICT 、加密、 MPEG 、 MIDI。
ASCII 格式和 EBCDIC，用于表示数字的 1S 或 2S 补码表示形式。

TELLIN 智能网系统
SMAP：业务管理接入点
SSP：业务交换点
业务管理接入点与业务交换点之间无连接

在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用三次握手建立一个连接。 第一次握手：建立连接时，客户端发送 syn 包(syn=j)到服务器，并进入 SYN_SEND 状态，等待服务器确认；第二次握手：服务器收到 syn 包，必须确认客户的 SYN（ack=j+1），同时自己也发送一个 SYN 包（syn=k），即 SYN+ACK 包，此时服务器进入 SYN_RECV 状态；第三次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(ack=k+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成三次握手。

文件传输协议（英文：File Transfer Protocol，缩写：FTP）是用于在网络上进行文件传输的一套标准协议。它属于网络传输协议的应用层。
FTP 是一个 8 位的客户端-服务器协议，能操作任何类型的文件而不需要进一步处理，就像 MIME 或 Unicode 一样。
TFTP 用作一个单纯的特殊用途文件传输协议。允许只能单向传输文件。
Telnet 协议是 TCP/IP 协议族的其中之一，是 Internet 远程登录服务的标准协议和主要方式，常用于网页服务器的远程控制，可供用户在本地主机运行远程主机上的工作。

协议是用来描述进程之间信息交换数据时的规则术语。在计算机网络中，两个相互 通信的实体处在不同的地理位置，其上的两个进程相互通信，需要通过交换信息来 协调它们的动作和达到同步，而信息的交换必须按照预先共同约定好的过程进行。 例如，网络中一个微机用户和一个大型主机的操作员进行通信，由于这两个数据终 端所用字符集不同，因此操作员所输入的命令彼此不认识。为了能进行通信，规定 每个终端都要将各自字符集中的字符先变换为标准字符集的字符后，才进入网络传 送，到达目的终端之后，再变换为该终端字符集的字符。当然，对于不相容终端， 除了需变换字符集字符外。敏感词特性，如显示格式、行长、行数、屏幕滚动方式等 也需作相应的变换。这样的协议通常称为虚拟终端协议。又如，通信双方常常需要 约定何时开始通信和如何通信，这也是一种协议。所以协议是通信双方为了实现通 信所进行的约定或对话规则。 计算机网络的协议主要由语义、语法和交换规则三部分组成，即协议三要素：
1.语义：规定通信双方彼此“讲什么”，即确定协议元素的类型，如规定通信双方要发出什么控制信息，执行的动作和返回的应答。
2.语法：规定通信双方彼此“如何讲”，即确定协议元素的格式，如数据和控制信息的格式。
3.交换规则：规定了信息交流的次序。

CLOSED：初始状态，表示没有任何连接。
LISTEN：Server 端的某个 Socket 正在监听来自远方的 TCP 端口的连接请求。
SYN_SENT：发送连接请求后等待确认信息。当客户端 Socket 进行 Connect 连接时，会首先发送 SYN 包，随即进入 SYN_SENT 状态，然后等待 Server 端发送三次握手中的第 2 个包。
SYN_RECEIVED：收到一个连接请求后回送确认信息和对等的连接请求，然后等待确认信息。通常是建立 TCP 连接的三次握手过程中的一个中间状态，表示 Server 端的 Socket 接收到来自 Client 的 SYN 包，并作出回应。
ESTABLISHED：表示连接已经建立，可以进行数据传输。
FIN_WAIT_1：主动关闭连接的一方等待对方返回 ACK 包。若 Socket 在 ESTABLISHED 状态下主动关闭连接并向对方发

送 FIN 包（表示己方不再有数据需要发送），则进入 FIN_WAIT_1 状态，等待对方返回 ACK 包，此后还能读取数据，但不能发送数据。在正常情况下，无论对方处于何种状态，都应该马上返回 ACK 包，所以 FIN_WAIT_1 状态一般很难见到。

FIN_WAIT_2：主动关闭连接的一方收到对方返回的 ACK 包后，等待对方发送 FIN 包。处于 FIN_WAIT_1 状态下的 Socket 收到了对方返回的 ACK 包后，便进入 FIN_WAIT_2 状态。由于 FIN_WAIT_2 状态下的 Socket 需要等待对方发送的 FIN 包，所有常常可以看到。若在 FIN_WAIT_1 状态下收到对方发送的同时带有 FIN 和 ACK 的包时，则直接进入 TIME_WAIT 状态，无须经过 FIN_WAIT_2 状态。

TIME_WAIT：主动关闭连接的一方收到对方发送的 FIN 包后返回 ACK 包（表示对方也不再有数据需要发送，此后不能再读取或发送数据），然后等待足够长的时间（2MSL）以确保对方接收到 ACK 包（考虑到丢失 ACK 包的可能和迷路重复数据包的影响），最后回到 CLOSED 状态，释放网络资源。

CLOSE_WAIT：表示被动关闭连接的一方在等待关闭连接。当收到对方发送的 FIN 包后（表示对方不再有数据需要发送），相应的返回 ACK 包，然后进入 CLOSE_WAIT 状态。在该状态下，若己方还有数据未发送，则可以继续向对方进行发送，但不能再读取数据，直到数据发送完毕。

LAST_ACK：被动关闭连接的一方在 CLOSE_WAIT 状态下完成数据的发送后便可向对方发送 FIN 包（表示己方不再有数据需要发送），然后等待对方返回 ACK 包。收到 ACK 包后便回到 CLOSED 状态，释放网络资源。

CLOSING：比较罕见的例外状态。正常情况下，发送 FIN 包后应该先收到（或同时收到）对方的 ACK 包，再收到对方的 FIN 包，而 CLOSING 状态表示发送 FIN 包后并没有收到对方的 ACK 包，却已收到了对方的 FIN 包。有两种情况可能导致这种状态：其一，如果双方几乎在同时关闭连接，那么就可能出现双方同时发送 FIN 包的情况；其二，如果 ACK 包丢失而对方的 FIN 包很快发出，也会出现 FIN 先于 ACK 到达。

使用 TCP 协议的常见端口主要有以下几种：

（1） FTP：定义了文件传输协议，使用 21 端口。常说某某计算机开了 FTP 服务便是
启动了文件传输服务。下载文件，上传主页，都要用到 FTP 服务。

（2）Telnet：它是一种用于远程登陆的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于 DOS 模式下的通信服务。如以前的 BBS 是纯字符界面的，支持 BBS 的服务器将 23 端口打开，对外提供服务。

（3）SMTP：定义了简单邮件传送协议，现在很多邮件服务器都用的是这个协议，用于发送邮件。如常见的免费邮件服务中用的就是这个邮件服务端口，所以在电子邮件设置中常看到有这么 SMTP 端口设置这个栏，服务器开放的是 25 号端口。

(4） POP3：它是和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议所用的是 110 端口。也是说，只要你有相应的使用 POP3 协议的程序（例如 Foxmail 或 Outlook），就可以不以 Web 方式登陆进邮箱界面，直接用邮件程序就可以收到邮件（如是 163 邮箱就没有必要先进入网易网站，再进入自己的邮箱来收信）。使用 UDP 协议端口常见的有：

（5）

HTTP：这是大家用得最多的协议，它就是常说的"超文本传输协议"。上网浏览网页时，就得在提供网页资源的计算机上打开 80 号端口以提供服务。常说"WWW 服务"、"Web 服务器"用的就是这个端口。

（6） DNS：用于域名解析服务，这种服务在 Windows NT 系统中用得最多的。因特网上的每一台计算机都有一个网络地址与之对应，这个地址是常说的 IP 地址，它以纯数字+"."的形式表示。然而这却不便记忆，于是出现了域名，访问计算机的时候只需要知道域名，域名和 IP 地址之间的变换由 DNS 服务器来完成。DNS 用的是 53 号端口。

（7） SNMP：简单网络管理协议，使用 161 号端口，是用来管理网络设备的。由于网络设备很多，无连接的服务就体现出其优势。

（8）

OICQ：OICQ 程序既接受服务，又提供服务，这样两个聊天的人才是平等的。OICQ 用
的是无连接的协议，也是说它用的是 UDP 协议。OICQ 服务器是使用 8000 号端口，侦听是否有信息到来，客户端使用 4000 号端口，向外发送信息。如果上述两个端口正在使用（有很多人同时和几个好友聊天），就顺序往上加。

在计算机的 6 万多个端口，通常把端口号为 1024 以内的称之为常用端口，这些常用端口所对应的服务通常情况下是固定的。表 1 所列的都是服务器默认的端口，不允许改变，一般通信过程都主要用到这些端口。

表 1

服务类型默认端口服务类型默认端口
Echo7 Daytime13
FTP21 Telnet23
SMTP25 Time37
Whois43 DNS53
Gopher70 Finger79
WWW80 POP3110
NNTP119 IRC194

另外代理服务器常用以下端口：
（1）. HTTP 协议代理服务器常用端口号：80/8080/3128/8081/9080
（2）. SOCKS 代理协议服务器常用端口号：1080
（3）. FTP 协议代理服务器常用端口号：21
（4）. Telnet 协议代理服务器常用端口：23

IPX:互联网数据包交换协议 ，(IPX:Internetwork Packet Exchange protocol)是一个专用的协议簇，它主要由 Novell NetWare 操作系统使用。IPX 是 IPX 协议簇中的第三层协议。
IPX 网络的地址长度为 80 位 (bit，由两部分构成，第一部分是 32 位的网络号，第二部分是 48 位的节点号。IPX 地址通常用十六进制数来表示。IPX 网络号是由网管人员分配的，可以根据需要来定义网络号。IPX 节点号通常是网络接口本身的 MAC 地址。

TCP/IP:
数据链路层：ARP,RARP
网络层： IP,ICMP,IGMP
传输层：TCP ,UDP,UGP
应用层：Telnet,FTP,SMTP,SNMP.

OSI:
物理层：EIA/TIA-232, EIA/TIA-499, V.35, V.24, RJ45, Ethernet, 802.3, 802.5, FDDI, NRZI, NRZ, B8ZS
数据链路层：Frame Relay, HDLC, PPP, IEEE 802.3/802.2, FDDI, ATM, IEEE 802.5/802.2
网络层：IP，IPX，AppleTalk DDP
传输层：TCP，UDP，SPX
会话层：RPC,SQL,NFS,NetBIOS,names,AppleTalk,ASP,DECnet,SCP
表示层:TIFF,GIF,JPEG,PICT,ASCII,EBCDIC,encryption,MPEG,MIDI,HTML
应用层：FTP,WWW,Telnet,NFS,SMTP,Gateway,SNMP

tcpdump 是简单可靠网络监控的实用工具
netstat 显示网络有关的信息，比如套接口使用情况、路由、接口、协议等
ifconfig 是查看活动的网卡信息
top 显示活动进程方面的情况

交换机可以隔离冲突域。是基于物理网卡地址的设备。交换机网络如果出问题，就会引发广播风暴。
路由器才能隔离广播域，当然冲突域也能隔离。是基于网络逻辑地址的设备。

巡警：110；
电话故障：112；
电话查询：114；
火警：119；

医疗急救：120；
天气预报：121
交通事故报警：122…

第四层即运输层，其中的 TCP 协议是具有流量控制，拥塞控制的面向对象的可靠数据传输协议，所以个人认为流量和拥塞控制可以对服务器和网络负载提供一个均衡的作用！

要明白这种攻击的基本原理，还是要从 TCP 连接建立的过程开始说起：
大家都知道，TCP 与 UDP 不同，它是基于连接的，也就是说：为了在服务端和客户端之间传送 TCP 数据，必须先建立一个虚拟电路，也就是 TCP 连接，建立 TCP 连接的标准过程是这样的：
首先，请求端（客户端）发送一个包含 SYN 标志的 TCP 报文，SYN 即同步（Synchronize），同步报文会指明客户端使用的端口以及 TCP 连接的初始序号；
第二步，服务器在收到客户端的 SYN 报文后，将返回一个 SYN+ACK 的报文，表示客户端的请求被接受，同时 TCP 序号被加一，ACK 即确认（Acknowledgment）。
第三步，客户端也返回一个确认报文 ACK 给服务器端，同样 TCP 序列号被加一，到此一个 TCP 连接完成。
以上的连接过程在 TCP 协议中被称为三次握手（Three-way Handshake）。
问题就出在 TCP 连接的三次握手中，假设一个用户向服务器发送了 SYN 报文后突然死机或掉线，那么服务器在发出 SYN+ACK 应答报文后是无法收到客户端的 ACK 报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送 SYN+ACK 给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度我们称为 SYN Timeout，一般来说这个时间是分钟的数量级（大约为 30 秒-2 分钟）；一个用户出现异常导致服务器的一个线程等待 1 分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源----数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的 CPU 时间和内存，何况还要不断对这个列表中的 IP 进行 SYN+ACK 的重试。实际上如果服务器的 TCP/IP 栈不够强大，最后的结果往往是堆栈溢出崩溃---即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的 TCP 连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从正常客户的角度看来，服务器失去响应，这种情况我们称作：服务器端受到了 SYN Flood 攻击（SYN 洪水攻击）。

电路交换是直接交换，分组交换采用存储转发的方式。因此电路交换时延更小。
分组交换的优点是可以实现链路复用

因为子网掩码的是 255.255.0.0，它没给网络地址，所以默认为 B 类 IP 地址，所以前 16 不变，后面只有在 0 到 255 都行。
1.又因为全 0 的主机号字段表示该 IP 地址是“本主机”所连接到的单个网络地址（如一主机 IP 地址为 5.6.7.8，则该主机所在的网络地址就是 5.6.0.0）。排除 A
2.而全 1 表示“所有的”，因此全 1 的主机号字段表示该网络上的所有主机。
（如 128.7.255.255 表示“在网络 128.7.0.0 上的所有主机”）排除 D

htons 把 unsigned short 类型从主机序转换到网络序
htonl 把 unsigned long 类型从主机序转换到网络序
ntohs 把 unsigned short 类型从网络序转换到主机序
ntohl 把 unsigned long 类型从网络序转换到主机序
WSANtohs() 将一个以网络字节顺序表示的无符号短整形数转换为主机字节顺序。

A，ping 命令用来检测两部主机之间的传输信道是否畅通，或远程主机是否正常
B，route 命令用来显示目前本机路由表的内容，并且还可以针对路由表中的记录来进行相应的添加、删除或修改等操作。
C，tracert 命令用来探测路由经过
D，ifconfig 命令用来来检测和设置本机的网络接口。

accept 发生在三次握手之后。
第一次握手：客户端发送 syn 包(syn=j)到服务器。
第二次握手：服务器收到 syn 包，必须确认客户的 SYN（ack=j+1），同时自己也发送一个 ASK 包（ask=k）。
第三次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(ack=k+1)。
三次握手完成后，客户端和服务器就建立了 tcp 连接。这时可以调用 accept 函数获得此连接。

ServerSocket (int port)
Creates a server socket, bound to the specified port.

Socket(InetAddress address, int port)
Creates a stream socket and connects it to the specified port number at the specified IP address.

一般网线两边头子是 586B 接线标准，特殊跳线一头是 586B，另一头一头 586A。
将两计算机通过双绞线直接连接就是一端是 586A，一端是 586B。
568A 标准：绿白，绿，橙白，蓝，蓝白，橙，棕白，棕
568B 标准：橙白，橙，绿白，蓝，蓝白，绿，棕白，棕
568A 和 568B 的标准就是把 1 和 3，2 和 6 的顺序换过来了，其他不变。
两台电脑直联,一头接 568A,一头接 568B，8 根线中 4，5，7，8 不用,只有橙白 1，橙 2，绿白 3，绿 6 四根线传数据。1，2 发数据,3，6 接收数据，所以必须 1，3 相接，2，6 相接，才能实现一头发数据，一头接收数据。若是 A 选项，则两头同时发送，同时接受，是会冲突的。

点对点协议(Point to Point Protocol)的缩写为 PPP,是 TCP/IP 网络协议包的一个成员。PPP 是 TCP/IP 的扩展,它增加了两个额外的功能组:
(1)它可以通过串行接口传输 TCP/IP 包;
(2)它可以安全登录。
当使用作为公共电话系统的部分的串行接口时,必须要注意确保所有通信的真实性。这个终端 PPP 集合了用户名字和密码安全。因此,一个路由器或者服务器通过 PPP 接收到一个请求时,如果这个请求的来源是不安全的,这就需要授权。这个授权是 PPP 的一部分。因为它的通过串行接口路由 TCP/IP 包的能力和它的授权能力,ISP (Internet 服务提供商)通常使用 PPP 来允许拨号用户连接到 Internet。

255 转换为 2 进制是 11111111
128 转换为 2 进制是 10000000
对地址 192.168.48.10 和掩码 255.255.255.128 进行 and 操作 得到 子网 192.168.48.0
ip 地址和掩码做 and 操作后， 得到这个子网地址的都属于这个 ip 段， 192.168.48.0 ... 192.168.48.127 和 255.255.255.128 进行 and 操作后都是 192.168.48.0
其中， 192.168.48.127 为广播地址， 192.168.48.0 ... 192.168.48.126 为有效地址

数据分段是在传输层中完成的，传输层定义了一些传输数据的协议和端口号（WWW 端口 80 等），如：TCP（传输控制协议，传输效率低，可靠性强，用于传输可靠性要求高，数据量大的数据），UDP（用户数据报协议，与 TCP 特性恰恰相反，用于传输可靠性要求不高，数据量小的数据，如 QQ 聊天数据就是通过这种方式传输的）。主要是将从下层接收的数据进行分段和传输，到达目的地址后再进行重组。常常把这一层数据叫做段。

虚拟局域网(VLAN)是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN 是一种比较新的技术，工作在 OSI 参考模型的第 2 层和第 3 层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点: 网络设备的移动、添加和修改的管理开销减少;可以控制广播活动;可提高网络的安全性。
在计算机网络中，一个二层网络可以被划分为多个不同的广播域，一个广播域对应了一个特定的用户组，默认情况

下这些不同的广播域是相互隔离的。不同的广播域之间想要通信，需要通过一个或多个路由器。这样的一个广播域就称为 VLAN。

A，查看帧中继网络的映射地址
B，查看 PVC 状态，pvc 有四种状态，分别是：delete，static，inactive，active。
C，查看本地路由和真交换机的状态消息数量，LMI 数据统计
D，查看接口的物理层和链路层信息，包括数据包的封装类型

广播地址(Broadcast Address)是专门用于同时向网络中所有工作站进行发送的一个地址。在使用 TCP/IP 协议的网络中，主机标识段 host ID 为全 1 的 IP 地址为广播地址，广播的分组传送给 host ID 段所涉及的所有计算机。例如，对于 10.1.1.0 （255.255.255.0 ）网段，其广播地址为 10.1.1.255 （255 即为 2 进制的 11111111 ），当发出一个目的地址为 10.1.1.255 的分组（封包）时，它将被分发给该网段上的所有计算机。

17 表示掩码前面有 17 位 1，后 15 位是 0 （总共 32 位）
10.1.0.1 跟 17 位 1 的掩码进行与操作 10 ， 1， 0， 1 各表示成 8 位的 2 进制 ， 得到 10.1.0.0
然后把 15 全部补成 1， 得到 10.1.127.255

POP3 协议用于接收或下载邮件，默认端口 110
SMTP 协议用于传输或发送邮件，默认端口 25
DNS 是域名解析的系统，默认端口 53
DHCP 是动态主机配置协议，默认端口 67（服务器）

GET:通过请求 URI 得到资源,POST:用于添加新的内容,OPTIONS:询问可以执行哪些方法,TRACE:用于远程诊断服务器,HEAD:类似于 GET, 但是不返回 body 信息，用于检查对象是否存在，以及得到对象的元数据
HEAD,GET,OPTIONS 和 TRACE 视为安全的方法，因为它们只是从服务器获得资源而不对服务器做任何修改，
但是 HEAD,GET,OPTIONS 在用户端不安全。而 POST 则影响服务器上的资源。

SYN: 表示建立连接
FIN: 表示关闭连接
ACK: 表示响应
PSH: 表示有 DATA 数据传输
RST: 表示连接重置。

VLAN 主要是限制网络上的广播，将网络划分为多个 VLAN 可减少参与广播风暴的设备数量。LAN 分段可以防止广播风暴波及整个网络。VLAN 可以提供建立防火墙的机制，防止交换网络的过量广播。使用 VLAN，可以将某个交换端口或用户赋于某一个特定的 VLAN 组，该 VLAN 组可以在一个交换网中或跨接多个交换机，在一个 VLAN 中的广播不会送到 VLAN 之外。同样，相邻的端口不会收到其他 VLAN 产生的广 播。这样可以减少广播流量，释放带宽给用户应用，减少广播的产生。

通信中规定长途自动接续中的忙音由发端的本地局收到终端忙信号后发出
第一层：物理层
第二层：数据链路层 802.2、802.3ATM、HDLC、FRAME RELAY
第三层：网络层 IP、IPX、APPLETALK、ICMP
第四层：传输层 TCP、UDP、SPX
第五层：会话层 RPC、SQL、NFS 、X WINDOWS、ASP
第六层：表示层 ASCLL、PICT、TIFF、JPEG、 MIDI、MPEG
第七层：应用层 HTTP,FTP,SNMP 等

TCP 是用面向连接的传输保证数据准确可靠的传输，对数据封装成 TCP 报文，每个 TCP 报文有编号，使用滑动窗口进行发送，接收 ACK 确认报文，以便接收端能够准确的恢复。

确认序列号=原始序列号+TCP 段的长度，所以第一次的确认序列号为 200+300=500，第二次确认序列号为 500+500=1000

ARP 和 RARP 是网络层的协议，但是它所工作的内容是链路层的。。。具体来说应该是在网络层。
地址解析协议（Address Resolution Protocol，ARP）是在仅知道主机的 IP 地址时确定其物理地址的一种协议。因 IPv4 和以太网的广泛应用，其主要用作将 IP 地址翻译为以太网的 MAC 地址，但其也能在 ATM 和 FDDIIP 网络中使用。从 IP 地址到物理地址的映射有两种方式：表格方式和非表格方式。ARP 具体说来就是将网络层（IP 层，也就是相当于 OSI 的第三层）地址解析为数据连接层（MAC 层，也就是相当于 OSI 的第二层）的 MAC 地址。

有关 tcp 连接握手
1. accept() api 调用发生在三次握手之后
2. “三次握手”的目的是“为了防止已失效的连接请求报文段突然又传送到了服务端，因而产生错误”
3. 因为 tcp 是全双工模式，接收到 FIN 时意味将没有数据再发来，但是还是可以继续发送数据，所以断开连接时必须是四次握手

connect 发送了一个 SYN，收到 Server 的 SYN+ACK 后，代表连接完成。发送最后一个 ACK 是 protocol stack,tcp_out 完成的。它是在三次握手过程中调用的。

DDN（Digital Data Network，数字数据网）是一种利用光纤、数字微波或卫星等数字传输通道和数字交叉复用设备组成的数字数据传输网。它的主要作用是向用户提供永久性和半永久性连接的数字数据传输信道，既可用于计算机之间的通信，也可用于传送数字化传真，数字话音，数字图像信号或其它数字化信号。永久性连接的数字数据传输信道是指用户间建立固定连接，传输速率不变的独占带宽电路。半永久性连接的数字数据传输信道对用户来说是非交换性的。但用户可提出申请，由网络管理人员对其提出的传输速率、传输数据的目的地和传输路由进行修改。网络经营者向广大用户提供了灵活方便的数字电路出租业务，供各行业构成自己的专用网。
ATM----Asynchronous Transfer Mode（ATM）异步传输模式的缩写。ATM 是一项数据传输技术，是实现 B-ISDN 的业务的核心技术之一。ATM 是以信元为基础的一种分组交换和复用技术，它是一种为了多种业务设计的通用的面向连接的传输模式。由于 ATM 网络是面向连接的，所以，在发送数据之前首先要发送一个分组以便建立连接，当这个初始分组经过子网的时候，该路径上所有的路由器都在他们的内部表中建立一个表项，用来标明该链接的存在，并且为它预留必要的资源。这里的链接通常称为虚电路（virtual circuit），类似于电话系统中使用的物理电路。
SDH（Synchronous Digital Hierarchy，同步数字体系），是不同速度的数位信号的传输提供相应等级的信息结构，包括复用方法和映射方法，以及相关的同步方法组成的一个技术体制。SDH 不仅适合于点对点传输，而且适合于多点之间的网络传输。SDH 传输网的拓扑结构，它由 SDH 终接设备(或称 SDH 终端复用器 TM)、分插复用设备 ADM、数字交叉连接设备 DXC 等网络单元以及连接它们的(光纤)物理链路构成。如果用于网络传输，则属于物理层，它需要物理连接。

会话跟踪常用的 4 种方法：URL 重写，隐藏表单域，cookie,sesion,URL 重写技术就是在 URL 结尾添加一个附加数据以标识该会话，把会话 ID 通过 URL 的信息传递过去，以便在服务端进行识别不同的用户，隐藏表单域：将会话 ID 添加到 HTML 表单元素中提交到服务器，此表单不再客户端显示，cookie,Cookie 是 Web 服务器发送给客户端的一小段信息，客户端请求时可以读取该信息发送到服务器端，进而进行用户的识别。对于客户端的每次请求，服务器都会将 Cookie 发送到客户端,在客户端可以进行保存,以便下次使用。 session: 在服务器端会创建一个 session 对象，产生一个 sessionID 来标识这个 session 对象，然后将这个 sessionID 放入到 Cookie 中发送到客户端，下一次访问时，sessionID 会发送到服务器，在服务器端进行识别不同的用户 , Session 是依赖 Cookie 的，如果 Cookie 被禁用，那么 session 也将失效

SNMP 为应用层协议，是 TCP/IP 协议族的一部分。它通过用户数据报协议(UDP)来操作。在分立的管理站中，管理者

进程对位于管理站中心的 MIB 的访问进行控制，并提供网络管理员接口。管理者进程通过 SNMP 完成网络管理。SNMP 在 UDP、IP 及有关的特殊网络协议(如，Ethernet, FDDI, X.25)之上实现。
所以依赖于 IP 和 UDP 协议。
简单 网络管理 协议（SNMP），由一组网络管理的标准组成，包含一个应用层协议（application layer protocol）、数据库模型（database schema）和一组资料物件。该协议能够支持网络 管理系统 ，用以监测连接到网络上的设备是否有任何引起管理上关注的情况。该协议是互联网工程工作小组（IETF，Internet Engineering Task Force）定义的 internet 协议簇的一部分。

A： HTTP（超文本传输协议）是一个基于请求与响应模式的、无状态的、应用层的协议。
B： 文件传输协议 FTP、电子邮件传输协议 SMTP、域名系统服务 DNS、HTTP 协议等都同是应用层协议。
C：HTTP 协议 状态代码有三位数字组成，第一个数字定义了响应的类别，且有五种可能取值：

1xx：指示信息--表示请求已接收，继续处理
2xx：成功--表示请求已被成功接收、理解、接受
3xx：重定向--要完成请求必须进行更进一步的操作
4xx：客户端错误--请求有语法错误或请求无法实现
5xx：服务器端错误--服务器未能实现合法的请求

常见状态代码、状态描述、说明：

200 OK //客户端请求成功
400 Bad Request //客户端请求有语法错误，不能被服务器所理解
401 Unauthorized //请求未经授权，这个状态代码必须和 WWW-Authenticate 报头域一起使用
403 Forbidden //服务器收到请求，但是拒绝提供服务
404 Not Found //请求资源不存在，eg：输入了错误的 URL
500 Internal Server Error //服务器发生不可预期的错误
503 Server Unavailable //服务器当前不能处理客户端的请求，一段时间后可能恢复正常

D： HTTP 是应用层协议，TCP，UDP 是传输层协议。

301，302 都是 HTTP 状态的编码，都代表着某个 URL 发生了转移，不同之处在于：
301 redirect: 301 代表永久性转移(Permanently Moved)，
302 redirect: 302 代表暂时性转移(Temporarily Moved)，

500 Internal Server Error 服务器遇到一个妨碍它为请求提供服务的错误时，使用此状态码
501 Not Implemented 客户端发起的请求超出服务器的能力范围（比如，使用了服务器不支持的请求方法）时，使用此状态码状态码 原因短语 含 义
502 Bad Gateway 作为代理或网关使用的服务器从请求响应链的下一条链路上收到了一条伪响应（比如，它无法连接到其父网关）时，使用此状态码
503 Service Unavailable 用来说明服务器现在无法为请求提供服务，但将来可以。如果服务器知道什么时候资源会变为可用的，可以在响应中包含一个 Retry-After 首部。更多有关 Retry-After 首部的信息请参见 3.5.3 节
504 Gateway Timeout 与状态码 408 类似，只是这里的响应来自一个网关或代理，它们在等待另一服务器对其请求进行响应时超时了
505 HTTP Version Not Supported 服务器收到的请求使用了它无法或不愿支持的协议版本时，使用此状态码。有些服务器应用程序会选择不支持协议的早期版本

物理层：RJ45、CLOCK、IEEE802.3
数据链路：PPP、FR、HDLC、VLAN、MAC
网络层：IP、ICMP、ARP、RARP、OSPF、IPX、RIP、IGRP

传输层：TCP、UDP、SPX
会话层：NFS、SQL、NETBIOS、RPC
表示层：JPEG、MPEG、ASII
应用层：FTP、DNS、Telnet、SMTP、HTTP、WWW、NFS

集线器工作在物理层，网桥工作在数据链路层
集线器工作在物理层。路由器工作在网络层。交换机工作在数据链路层

物理层：通过媒介传输比特,确定机械及电气规范（比特 Bit）
数据链路层：将比特组装成帧和点到点的传递（帧 Frame）
网络层：负责数据包从源到宿的传递和网际互连（包 PackeT）
传输层：提供端到端的可靠报文传递和错误恢复（段 Segment）
会话层：建立、管理和终止会话（会话协议数据单元 SPDU）
表示层：对数据进行翻译、加密和压缩（表示协议数据单元 PPDU）
应用层：允许访问 OSI 环境的手段（应用协议数据单元 APDU）

UDP 报头只有四个域：源端口号，目的端口号，数据报长度，检验和。

网络层---数据包的包格式里面有个很重要的字段叫做协议号。比如在传输层如果是 TCP 连接，那么在网络层 IP 包里面的协议号就将会有个值是 6，如果是 UDP 的话那个值就是 17---传输层。
传输层---通过接口关联(端口的字段叫做端口)---应用层。
用 netstat －an 可以查看本机开放的端口号。
代理服务器常用以下端口：
（1）. HTTP 协议代理服务器常用端口号：80/8080/3128/8081/9080
（2）. SOCKS 代理协议服务器常用端口号：1080
（3）. FTP（文件传输）协议代理服务器常用端口号：21
（4）. Telnet（远程登录）协议代理服务器常用端口：23

WIN2003 远程登陆，默认的端口号为 3389；
DHCP server 的端口号是 67
端口号的范围是从 1～65535。其中 1～1024 是被 RFC 3232 规定好了的，被称作“众所周知的端口”(Well Known Ports)；从 1025～65535 的端口被称为动态端口（Dynamic Ports），可用来建立与其它主机的会话，也可由用户自定义用途。
一些常见的端口号及其用途如下：
TCP 21 端口：FTP 文件传输服务
TCP 23 端口：TELNET 终端仿真服务
TCP 25 端口：SMTP 简单邮件传输服务
UDP 53 端口：DNS 域名解析服务
TCP 80 端口：HTTP 超文本传输服务
TCP 110 端口：POP3 “邮局协议版本 3”使用的端口
TCP 443 端口：HTTPS 加密的超文本传输服务
TCP 1521 端口：Oracle 数据库服务
TCP 1863 端口：MSN Messenger 的文件传输功能所使用的端口
TCP 3389 端口：Microsoft RDP 微软远程桌面使用的端口
TCP 5631 端口：Symantec pcAnywhere 远程控制数据传输时使用的端口
UDP 5632 端口：Symantec pcAnywhere 主控端扫描被控端时使用的端口
TCP 5000 端口：MS SQL Server 使用的端口
UDP 8000 端口：腾讯 QQ

TCP 25 端口：SMTP 25 仔
TCP 110 端口：POP3 报警 110 police

常见的网络协议\端口号
一个网络协议至少包括三要素:
语法 用来规定信息格式；数据及控制信息的格式、编码及信号电平等。
语义 用来说明通信双方应当怎么做；用于协调与差错处理的控制信息。
时序（定时 ）详细说明事件的先后顺序；速度匹配和排序等
网际(络)层协议：包括：IP 协议、ICMP 协议、ARP 协议、RARP 协议。
传输层协议：TCP 协议、UDP 协议。
应用层协议：FTP、Telnet、SMTP、HTTP、RIP、NFS、DNS。

使用 TCP 协议的常见端口主要有以下几种：
（1）
FTP：定义了文件传输协议，使用 21 端口。常说某某计算机开了 FTP 服务便是启动了文件传输服务。下载文件，上传主页，都要用到 FTP 服务。
（2）
Telnet：它是一种用于远程登陆的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于 DOS 模式下的通信服务。如以前的 BBS 是纯字符界面的，支持 BBS 的服务器将 23 端口打开，对外提供服务。
（3）
SMTP：定义了简单邮件传送协议，现在很多邮件服务器都用的是这个协议，用于发送邮件。如常见的免费邮件服务中用的就是这个邮件服务端口，所以在电子邮件设置中常看到有这么 SMTP 端口设置这个栏，服务器开放的是 25 号端口。
（4）
POP3：它是和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议所用的是 110 端口。也是说，只要你有相应的使用 POP3 协议的程序（例如 Foxmail 或 Outlook），就可以不以 Web 方式登陆进邮箱界面，直接用邮件程序就可以收到邮件（如是 163 邮箱就没有必要先进入网易网站，再进入自己的邮箱来收信）。
使用 UDP 协议端口常见的有：
（1）
HTTP：这是大家用得最多的协议，它就是常说的"超文本传输协议"。上网浏览网页时，就得在提供网页资源的计算机上打开 80 号端口以提供服务。常说"WWW 服务"、"Web 服务器"用的就是这个端口。
（2）
DNS：用于域名解析服务，这种服务在 Windows
NT 系统中用得最多的。因特网上的每一台计算机都有一个网络地址与之对应，这个地址是常说的 IP 地址，它以纯数字+"."的形式表示。然而这却不便记忆，于是出现了域名，访问计算机的时候只需要知道域名，域名和 IP 地址之间的变换由 DNS 服务器来完成。DNS 用的是 53 号端口。
（3）
SNMP：简单网络管理协议，使用 161 号端口，是用来管理网络设备的。由于网络设备很多，无连接的服务就体现出其优势。
另外代理服务器常用以下端口：
（1）. HTTP 协议代理服务器常用端口号：80/8080/3128/8081/9080
（2）. SOCKS 代理协议服务器常用端口号：1080
（3）. FTP 协议代理服务器常用端口号：21

（4）. Telnet 协议代理服务器常用端口：23