香农定理与奈奎斯特定理问题：

数据速率即数据传输率，是单位时间内在信道上传送的信息（位数）。

香农定理

香农定理总结出有噪声信道的极限数据速率：在一条带宽为 W（HZ），信噪比为 S/N 的有噪声信道的极限数据速率 Vmax 为：

$$Vmax=W \log2(1+S/N) \quad 单位(b/s)$$

分贝与信噪比的关系为：

$$dB=10\log10S/N \qquad dB 的单位为 分贝$$

例：设信道带宽为 4kHz，信噪比为 30dB，按照香农定理，信道的最大数据传输速率约等于？

解：1，根据题意例出香农定理算式：Vmax=Wlog2(1+S/N)

2, 例出信噪比关系：dB=10log10S/N

3, 计算 30dB=10log10S/N 则 S/N=1000

4，Vmax=4Khz log2(1+1000)=4000x10 =40000b/s=40kb/s

注意：此处出现单位换算一次，1 kb/S=1000b/s

尼奎斯特定理

有限带宽无噪声信道的极限波特率，成为尼奎斯特定理，若信道带宽为 W（HZ）,则最大码元速率（波特率）为：

$$B=2W（baud）$$

码元的信息量 n 与码元的种类数 N 有如下关系，数据速率= 码元速率(波特率)*码元携带的信息量

$$n=\log2N$$

所以，由尼奎斯特定理可得：

$$Vmax=B \text{ long}2N=2 w \log2N \quad 单位（b/s）$$

例：设信道带宽为 3400Hz，调制为 4 种不同的码元，根据 Nyquist 定理，理想信道的数据速率为？

解：1，根据题意例出尼奎斯特定理算式：Vmax=2 W long 2N

2, 直接套入数字：Vmax=2x3400xlog2(2 次方)

3, Vmax=2x3400x2=13600b/S=13.6kb/s

注意：此处出现单位换算一次，13600b/s=13.6kb/2

例 1：设信道采用 2DPSK 调制，码元速率为 300 波特，则最大数据速率为

解：Vmax=B long2N=300x1=300b/s

例 2：在异步通信中，每个字符包含 1 位起始位，7 位数据位，1 位奇偶效验位和两位终止位，若每秒传送 100 个字符，采用 4DPSK 调制，则码元速率为？有效数据速率为？

解：1，根据题意计算数据速率为 （1+7+1+2）*100=1100b/s

2，由尼奎斯特定理得出，1100b/s=B*log2^4

3，B=1100/2=550baud

4, 有效数据速率，即单位时间内传输的数据位，即 7*100=700b/S

E1 与 T1 问题

E1 载波基本帧由 32 个子信道组成，其中 30 个子信道用于传送话音数据，2 个子信道 CH0 和 CH16 用于传送控制命令，该基本帧的传送时间为 125us。
在 E1 载波中，每个子信道的数据速率是 64Kb/s，E1 载波的控制开销占 6.25%
E1 信道的数据速率是 2.048Mb/s
T1 载波的每个信道的数据速率为 64kb/s，T1 信道的总数据速率是 1.544Mb/s
E3 的数据速率是 34.368Mb/s ，T3 信道的数据速率为 44.736Mb/s

HDLC
高级数据链路控制协议是一种面向比特的同步链路控制协议，采用 01111110 作为标志以确定帧的边界。

数据传输延迟问题

总延迟 T=发送延迟 T1+传输延迟 T2
注意：电信号在电缆上传播的速度为光速的 2/3，即 20wkm/s
　　卫星传送信号的延迟恒定为 270ms
例：在相隔 2000km 的两地间通过电缆以 4800b/s 的速率传送 3000 比特长的数据包，从开始发生到接收数据需要的时间是:？，如果用 50Kb/s 的卫星信道传送，则需要的时间是？
解：
对于电缆：
　传输延迟 T1=2000km/(20km/ms)=10ms
　发送延迟 T2=3000b/(4800b/s)=625ms
　T=T1+T2=625ms+10ms=635ms
对于卫星：
　传输延迟 T1=270ms
　发送延迟 T2=3000 b/(50kb/s)=60ms
　T=T1+T2=270ms+60ms=330ms
注意：卫星传输数据时与地面相隔距离无关。

数字化技术 PCM 计算问题

PCM 主要经过 3 个过程：**采样，量化和编码。**

$$f=1/T\geq 2f_{max}$$

f 为采样频率，T 为采样周期， fmax 为信号的最高频率。
例：设信道带宽为 3400HZ，采用 PCM 编码，采样周期为 125μs，每个样本量化为 128 个等级，则信道的数据速率为？
解：f=1s/125us=8000Hz
　8000Hz＞3400Hz*2
　128=2 的 7 次方
　则：数据速率=8000Hz*7=56000b/S=56kb/s

CSMA/CD 以太帧最小帧长计算问题

最小帧长与数据速率的比值必须大于等于传输距离与传输速率的比值

设 L 为最小帧长，R 为数据速率，S 为两端距离，V 为传输速度，则

$$L/R \geq 2（S/V）$$

例，一个运行 CSMA/CD 的协议的以太网，数据速率为 1GB/S，网段长 1KM，

信号速度为 200000KM/S，则最小帧长度为？

解，L/R≥2(S/V)

即 L/1(gb/s)=2x(1km/20000(m/s))

即 L=10000b

注意单位换算问题

1GB/S=1000 000 000b/s

CSMA/CD 考点汇总：

CSMA/CD（Carrier Sense Multiple Access/Collision Detect）即载波监听多路访问/冲突检测机制。CSMA/CD 采用一种称为二进制后退算法，这种方法在重负荷时仍能保证系统的稳定性，有效分解冲突。

CSMA/CD，不适于所有 802.3 以太网，在 10 千兆位以太网就忽略了 CSMA/CD。

非坚持的 CSMA：线路忙，等待一段时间，再侦听；不忙时，立即发送；减少冲突，信道利用率降低：

1 坚持的 CSMA：线路忙，继续侦听；不忙时，立即发送；提高信道利用率，增大冲突：

p 坚持的 CSMA：线路忙，继续侦听；不忙时，根据 p 概率进行发送，另外的 1-p 概率为继续侦听（p 是一个指定概率值）；有效平衡，但复杂：

CSMA/CA 考点汇总

CSMA/CA：带有冲突避免的载波侦听多路访问，发送包的同时不能检测到信道上有无冲突，只能尽量避免。

所有站在完成发送后，必须再等待一段很短的时间（继续监听）才能发送下一帧。这段时间成为帧间间隔 IFS（inter frame space），每一个发送站维持一个后退计算器，并监听网络上的通信。

CSMA/CA 协议适用于突发性业务。

各个发送站在两次帧间间隔（IFS）之间进行竞争发送。

OSI/RM 各层功能简介

7、应用层	application layer	处理网络应用
6、表示成	presentation layer	数据表示，数据压缩
5、会话层	session layer	互联主机通信
4、传输层	transport layer	端到端应带，分组排序，流量控制
3、网络层	network layer	分组传输和路由选择
2、数据链路层	data link layer	传送以帧为单位的信息
1、物理层	physical layer	二进制数据传输

各协议注意事项：

网络层的服务访问点是 ip 地址。

BGP 协议是一种路由协议，BGP 报文封装在 TCP 报文中，

BGP 报文类型有：建立邻居关系的 open，对 open 请求应答的 keepalive，发送路由更新的 update 报文，通告路由错误的 notification 报文。

ICMP 工作在网络层，ICMP 报文封装在 IP 数据报中传输，是一种面向连接。

ICMP 报文用于测试目的主机或路由器是否可达，回声请求用于确实是否连通，路由重定向即更改路由器的跳步顺序。

SNMP 基于 UDP 传输方式。

TFTP 提供不可靠的数据流传输服务，承载在 UDP 上。

ARP 和 RARP 协议，在 TCP/IP 协议族中属于网络层，在 OSI 模型中属于数据链路层，ARP 报文封装在以太帧中。

使用 ADSL 拨号上网，需要在用户端安装 ARP 协议来建立 IP 地址到 MAC 地址间的映射。

TCP 报头的最小长度是 20 字节。

在 TCP 协议中，采用端口号来区分不同的应用进程。

TCP 进行流量控制的方法是使用可变大小的滑动窗口协议。

在 TCP/IP 网络中，为各种公共服务保留的端口号为 1-1023。

127.0.0.1 是 IPV4 环回地址，它被分配给了一个内部环回接口，此接口可供节点用来向自己发送数据包。该地址既可以作为目标地址，也可以作为源地址。

自动专用 IP 地址（automatic private ip address APIPA）地址范围是 169.254.0.0-169.254.255.255，在网络故障找不到 DHCP 服务器或 DHCP 服务器失效时使用。

如果帧编号字段为 K 位，对于选择重发 ARQ 协议，发送窗口大小为 W≤2 的 K-1 次方，对于后退 N 帧的 ARQ 协议，则窗口大小为 W≤2 的 K 次方-1。

Ipv4 协议头中标识符字段的作用是用于分段和重装。

当 TCP 实体要建立连接时，其段头中的 SYN 标识置 1。

UDP 协议在 IP 层上提供了端口寻址功能。

Ipv6 协议数据单元表示松散源路由功能的扩展头部是路由选择头部，如果有多个扩展头部，第一个扩展头部为逐条头部。

Ipv6 中，地址类型由格式前缀来区分，Ipv6 可集聚全球单播地址的格式前缀是 001

Ipv6 中，0:0:0:0:0:0:0:0 表示不确定地址，不能分配给任何节点，0:0:0:0:0:0:0:1 表示回环地址，节点用这种地址向自身发送 ipv6 分组

Ipv6 的“链路本地地址”是将主机的 MAC 地址附加在地址前缀 1111 1110 10 之后产生的。

telnet 采用客户端/服务器工作方式，采用 NVT（网络虚拟终端）格式，实现客户端和服务器的数据传输。

DNS 服务器中，主域名服务器具有一个或几个域的授权，并负责维护这个区域的所有域名信息。辅助域名服务器作为主域名服务器的备份服务器提供域名解析服务。转发域名服务器主要负责非本地域名的查询。缓存域名服务器可以通过自己的查询操作建立地址缓存的服务器，它没有域名数据库。任何一个 internet 用户可以使用整个域名树上的任何一个域名服务器来解析域名。

在域名解析过程中，缓存域名服务器获取的解析结果耗时最短。

DNS 服务器在名称解析过程中正确的查询顺序是 本地缓存记录→区域记录→转发域名服务器→根域名服务器。

DNS 服务器进行域名解析时，采用递归方法，发送域名请求为 1 条，迭代则是多条。

DNS 资源记录中记录类型（record-type）有多种，SOA 是授权，NS 是域名，A 是 IP 地址，CNAME 是别名，MX 是邮件，PTR 是指针。

DNS 中，没有域名数据库的是缓存域名服务器。

ftp 命令中，用来设置客户端当前工作目录的命令是 lcd。

http 协议中，用来读取一个网页的操作方法是 GET。

应用层	HTTP、FTP、telnet、SMTP	SNMP、DNS、DHCP
	POP、DNS	TFTP
传输层	TCP	UDP
网络层	IP、ICMP、ARP、RARP	
通信子网层	电话网，局域网，无线网	

常见协议的端口号：

FTP 20 数据 21 控制 ，FTP 协议中，控制连接是由客户端主动建立的，是服务器客户端程序。

telnet23，为了使异构计算机和操作系统间的 Telnet 交互操作成为可能，Telnet 协议定义了一种通用字符终端作为数据和命令在 Internet 上的传输方式，即 NVT（Net Virtual Terminal，网络虚拟终端）

smtp25，DNS53（TCP 和 UDP 都它都能用） TFTP69， HTML80，SNMP161。 DHCP67、68 ，DHCP 客户端不能从 DHCP 服务器获得 web 服务器的 IP 地址。

Pop3 协议采用 Client/server 模式，客户端与服务器建立 TCP 连接，占用 TCP 端口 110。

HTTPS 是一种安全的 HTTP 协议，它使用 SSL 来保证信息安全，使用 TCP 的 443 端口来发送和接收报文。HTTPS 安全机制工作在传输层。

SSL：secure socket layer 是目前解决传输层安全问题的一个主要协议，基于 TCP 协议上提供可靠的端到端安全服务，SSL 协议使用的默认端口是 443

IPSEC，通过扩充认证头 AH 及对报文内容进行加密封装 ESP 有效的保障网络安全。IPSEC 是网络层安全协议。

TLS(transport layer security) 传输层安全协议，是确保互联网上通信应用和其用户隐私的协议，TLS 由两层构成，TLS 记录协议和 TLS 握手协议，TLS 属于传输层安全协议。

报文摘要算法 MD5 的输出是 128 位，SHA-1 的输出是 160 位。

SNMP：simple network management protocol ,简单网络管理协议，端口 161，用来对通信线路进行管理，SNMP service 为 windows 发送 SNMP 请求报文，并能对 SNMP 报文进行解析服务，而 SNMP trap service （trap[陷阱]）用以监听被管主机发送来的陷入报文的服务。

PGP(Pretty Good Privacy)，是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。

DNS，是域名系统（Domain Name System）的缩写，它是因特网的一项核心服务，它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串，使用端口 53.

DNS 查询模式

1.递归查询:

一般客户机和服务器之间属递归查询，即当客户机向 DNS 服务器发出请求后,若 DNS 服务器本身不能解析,则会向另外的 DNS 服务器发出查询请求，得到结果后转交给客户机；

2.迭代查询(反复查询):

一般 DNS 服务器之间属迭代查询，如：若 DNS2 不能响应 DNS1 的请求，则它会将 DNS3 的 IP 给 DNS2，以便其再向 DNS3 发出请求；

RIP 每 30 秒，IGRP 每 90 秒一次发布路由更新。OSPF 不论是否网络拓扑发生改变，每 10 秒发送一次 hello 数据包，OSPF 如果 40 秒没有收到 hello 分组，就认为对方不存在。

IGRP(interior gatway routing protocol)内部网关路由协议，是一种动态距离向量路由协议，由思科设计，使用组合用户配置尺度，包括带宽，延迟，可靠性和最大传输单元 (MTU)。

IGRP 协议的路由度量一般情况下可以简化为跳步数。

默认情况下，IGRP 每隔 90 秒发送一次路由更新广播，在 3 个更新周期内（270 秒），没有从路由中的第一个路由器接收到更新，则宣布路由不可访问。

IGRP 配置为：

Router(config)#router igrp 10

Router(config)-router)#network 192.168.20.0

IGRP 不支持可变长子网掩码

RIPV1 与 RIPV2

RIPV2 是一个距离矢量路由协议，相比 RIPV1 具有三处改进：

1，使用组播而不是 RIPV1 的广播来传播路由更新。

2，采用触发更新机制来加速路由收敛，即出现变化时向邻居发送更新报文，可以不必等待更新周期。

3，支持无类域间路由 CIDR，使网络设计更加具有伸缩性。

RIPV1 与 V2 具有共同点是，以跳步数来度量路由费用，允许最大跳步数为 15 跳。

OSPF：开放最短路径路由协议

OSPF 是链路状态路由协议，在同一层的区域内与其他所有路由器交换链路状态公告（LSA）信息。OSPF 的工作是有层次的，其层次中最大实体为自制系统（AS）。AS 是遵循共同路由策略统一管理下的网络群，拥有多个接口的路由器可以加入多个区间，这些路由器成为边缘路由器，分别为每个区间保存其拓扑数据库。

OSPF 主干负责在区间分发路由信息，包含所有的区间边缘路由器，非全部属于某区间的网络及其相连的路由器。

SPF 算法是 OSPF 的基础，用 OSPF hello 协议来获取邻居信息，hello 包也含有 keepalive 功能。自治系统号由 16 比特组成，共有 65533 个取值。

OSPF 采用 Hello 协议分组来维持与邻居的连接，采用 LSA（链路状态广播信息）和这些路由器交换链路状态信息。在默认情况下，40 秒没有收到 hello 分组，就认为对方不存在。

每一个路由器都包含同一 AS 种的数据库项

在同一区域中，所有 OSPF 路由器都维护一个相同的 AS 结构数据库。使用 Dijkstra 算法来计算每一个目的路由器的距离。

使用 LSA(link state adrertsement)链路状态通告来更新和维护拓扑数据库。

BGP(Bord Gateway protocol)边界网关协议，是运行在 TCP 上的一种自治系统的路由协议，采用触发性的路由更新机制，不交换整个 BGP 表，而只更新发生变化的路由条目。路由更新是由 update 消息来完成的，当没有路由更新传送时，BGP 会话用 keepalive 消息来验证连接的可用性。Keepalive 包很小，可以节省带宽，协商发生错误时，BGP 会向双方发送 notification 消息来通知错误。

在 BGP 协议中，open 报文用于与相邻的另一个 BGP 发言人建立相邻关系，update 报文用于确认 open 报文，以及周期性证实相邻边界路由的存在，notification 用于发送检测到的差错，BGP 支持 CIDR，拥有丰富的路由过滤和路由策略。

STP：spanning tree protocol 生成树协议，STP 要求每个网桥分配一个唯一的标识（BID），BID 通常由优先级（2 bytes）和网桥 MAC 地址（6bytes）构成。
交换机优先级以 4096 为块大小递增或递减，默认值为 32768。根据选举规则，选择较小的交换机，当优先级相同的时候，查找最小的 MAC 地址成为根交换机。

MPLS 多协议标签交换，是一种快速数据包交换和路由的体系，它为网路哦数据流量提供了目标路由，转发和交换等能力，它拥有管理不同形式通信流的机制。
MPLS 网络由核心部分的标签交换路由器 LSR 和边缘部分的标签边缘路由器 LER 组成。

LER 的作用是分析 IP 包头，决定相应的传送级别和标签交换的路径 LSP

MPLS 工作流程：
1、由 LDP(标签分发协议)和传统路由协议(ospf)等在 LSR 中建立路由表和标签映射表。
2、在 MPLS 出口处的 LER 接收 IP 包，完成三层功能，并给 IP 包打上标签。
3、在 MPLS 出口处的 LER 将分组中的标签去掉后继续转发。
4、LSR 不再对分组进行第三层处理，只根据分组上的标签交换单元进行转发。

MPSL 格式　2 层头部###MPLS 头部###ip 头部###数据
严格源路由选项规定，IP 数据报要经过路径上的每一个路由器，相邻路由器间不得有中间路由器，并且所经过的路由器顺序不可更改，而松散源路由选项只会给出 IP 数据报必须经过源站指定的路由器，并不给出一条完备的路径，即松散源路由指 IP 分组必须经过源站指定的路由器，不规定路径。

交换机

交换机有三种交换方式：存储转发交换，直通交换，碎片过滤式交换。

STP：spanning tree protocol 生成树协议，STP 要求每个网桥分配一个唯一的标识（BID），BID 通常由优先级（2 bytes）和网桥 MAC 地址（6bytes）构成。

交换机优先级以 4096 为块大小递增或递减，默认值为 32768。根据选举规则，选择较小的交换机，当优先级相同的时候，查找最小的 MAC 地址成为根交换机。

IEEE802.1d 协议，就是生成树协议，所有网桥有 5 种状态功能。

阻塞(blocking)不转发器，不学习

监听(listening)识别根桥，可区分根端口，指定端口，和非指定端口，不能学习接收帧的地址。

学习(learning)MAC 端口能够学习接收帧的 MAC 地址，但不能转发。

转发(orwarding)MAC 端口可以学习接收帧的源地址，并可以根据目的地址将其转发到适当的端口。

禁用(disabled)MAC 端口不参与生成树算法。

VTP 协议，交换机的运行模式可分为 3 种：

1、服务器模式(server)，可以创建，添加，删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机，一个管理域中可以有多个服务器。

2、客户机模式(clien)不允许创建，修改或删除 VLAN，但可以监听并据此修改自己的 VLAN。

3、透明模式(transporent)可进行 VLAN 配置，但配置信息不会传播至其他交换机。

网络分类

IEEE802.3ae 10Gb/s 以太网，10Gb/s 以太网中，全部采用光纤标准，不再支持半双工模式，一律全双工。

IEEE802.3 规定的最小帧长为 64 字节，这个帧长是指从目标地址到校验和的长度。

千兆以太网标准 802.3z 定义了一种帧突发方式（frame bursting），这种方式是指一个站可以连续发送多个帧

Ethernet 数据帧格式最多 1518 字节，目的 MAC6 字节，源 MAC6 字节，类型 2 字节，CRC4 字节，剩下为数据部分的 1500 个字节，其中，IP 头 20 字节，TCP 头 20 字节，则数据部分最长为 1460 字节。

8021.q 封装协议，在原来的以太帧头中的源地址后增加了一个 4 字节的 802.1q 标签。

IEEE 802.11 标准定义的 Peer to Peer 网络是一种不需要有线网络和接入点支持的点对点网络。

以太网协议中使用二进制后退算法，该算法的最大特点是在重负载下，提高网络的利用率。

IEEE802.11 标准定义了两种无线网络的拓扑结构，一种是基础设施网络，它通过无线接入点 AP 将其连接到现在网络。二是特殊网络 AD HOC，它是一种点对点连接。

IEEE802.11	标准	速度	技术
802.11	2.4GHZ，ISM 频段	1mb/s，2mb/s	扩频通信技术
802.11b	2.4GHZ，ISM 频段	11mb/s	Cck 技术
802.11a	5GHZ，U-NII 频段	54mb/s	OFDM 调制技术
802.11g	2.4GHZ,ISM 频段	54mb/s	OFDM 调制技术
802.11n	智能无线技术	300mb/s→600mb/s	MIMO 与 OFDM 技术

IEEE 802.11i 规定使用 802.1x 认证和密钥管理方式，在数据加密方面，定义了 TKIP（Temporal Key Integrity Protocol）、CCMP（Counter-Mode/CBC-MAC Protocol）和 WRAP（Wireless Robust Authenticated Protocol）三种加密机制

802.11i 采用加密算法为 AES。

802.11b 定义无线网络安全协议 WEP，是一种 MAC 层认证机制，使用 RC-4 加密法，是对称加密

机制，长度为 40 或 128 位。

IEEE802.11 标准使用扩频通信技术，即使用伪随机序列，对代表数据的模拟信号进行调制。

帧中继的地址格式中，表示虚电路标识符是 DLCI。

组网技术中，家庭局域网不但能够连接因特网，而且 WLAN 内部还可以直接通信，应使用设备为无线路由器+无线网卡。

使用代理服务器不能避免来自 internet 上病毒的入侵，不能对信息加密。

网路结构的三层模型细节：

接入层：实现用户访问，要求成本低，高密度，接入层可实现用户访问控制即 MAC 绑定。

汇聚成：分为多个广播/组播域，可以实现 VLAN 间的路由选择，并通过访问控制列表实现分组过滤。

核心层：主干线路，提供链路冗余，路由冗余，VLAN 中继和负载均衡等功能。

网络通信设备

多模光纤与单模光纤的特殊区别：

多模光纤使用发光二极管，单模光纤使用激光二极管。

多模光纤允许多束光纤穿过光纤，单模光纤比多模光纤采用的波长长。

单模光纤只允许一束光线穿过光纤，单模光纤传输频带宽，多模光纤传输频带窄。

局域网中双绞线可分为非屏蔽双绞线(UTP)和屏蔽双绞线(STP)两类，STP 有金属包层，辐射小，价格高。

UTP 分为 3 类，4 类，5 类和超 5 类 4 种。

3 类 UTP 适应以太网(10mb/s)对传输介质的要求。(4 类与 3 类差不多)

5 类 UTP 因价廉质优为快速以太网(100Mb/s)首选。

超 5 类 UTP 为千兆以太网(1000Mb/s)

100BASE－TX 是一种以太网标准，用于描述 5 类非屏蔽双绞线上如何运行 100Mb/s 速率的快速以太网，100BASE 使用两对抗阻为 100 欧姆的 5 类非屏蔽双绞线，最大传输距离为 100 米一对用于发送，一对用于接收，用 4B/5B 编码方式，自动协商最大传输速率。

IEEE 802.3au

100BASE-TX	5 类非屏蔽双绞线	2 对跳线	传输距离 100m
100BASE-FX	62.5/125 多模光纤	2 对用于收发	传输距离 400m
100BASE-T4	3 类非屏蔽双绞线	4 对用于收发	传输距离 100m

光纤覆盖分类（FTTX）：

FTTN，光纤到节点即光纤到弱电箱。【node 节点】

FTTC，光纤到路边。【curb】路边

FTTZ，光纤到小区。【zone】地区

FTTH，光纤到户。【home】户

光纤布线系统测试指标包括：最大衰减值，波长窗口参数，回波损耗限值，与近端串扰无关，近端串扰用于测试双绞线。

通常请了下，信息插座安装在距离地面 30→50CM 高。

ADSL 接入方式分为虚拟拨号和准专线两种。

采用虚拟拨号的用户需安装 PPPOE 或 PPPOA 客户端软件，以及类似于 MODEM 的拨号程序，输入用户名称和用户密码即可接到宽带接入点。

采用准专线方式的用户使用电信部门静态或动态分配的 IP 地址，开机即可接入 internet。

家庭内，PC 通过 ADSLMODEM→分离器→入户接线盒→电话线→DSL 接入复用器(DSLAM)连接 ATM 或 IP 网络。

话音线路通过：分离器→入户接线盒→电话线→DSL 接入复用器，接入电话交换机。

局域网管理站轮询问题：最大支持设备=轮询时间（秒）÷一次查询时间（秒）

例如：假设某局域网，管理站每 15min 轮询管理设备一次，一次查询时间是 200MS。则管理站最多可支持 15*60/0.2=4500 个。

计算机病毒

1、蠕虫是一种常见的病毒，主要通过网络和电子邮件传播。
2、目录行病毒，可改变相关目录的文件项。
3、引导型病毒，寄生于主引导区，引导区，病毒利用操作系统的引导模块放在某个固定位置，将移动引导分区内容。
4、多型病毒，每次感染都会改变自己。
5、特洛伊木马，特征为有未知程序试图建立网络连接。

各种病毒的名称：

Worm .sasser 蠕虫
Troian.qq psw 特洛伊木马
Backdoor.IRCBot 后门
Macro .Melissa 宏病毒

网络安全

PPP：point-to-point protocol 点对点协议

建立 PPP 链接以后，发送方就发出一个提问消息(challenge[挑战] message)，接收方根据提问消息来计算一个散列值，CHAP 协议采用这种方式进行用户认证。

CHAP：challeng handshake authentication protocol 挑战握手协议，通过三次握手周期性地校验对端的身份，在初始链路完成时，可以在链路建立之后的任何时候重复进行，具体过程为：

1、链路建立，以认证者向对端发送 challenge 消息。
2、对端点用经过担心哈希函数来应答。
3、认证者根据自己计算的哈希值来应答，配对则承认。
4、经过一段时间发送新的 challenge 给端点。

PKI （Pubic Key Infrastructure）公钥基础设施，是一组规则，过程，人员，设施，软件和硬件的集合。可用来进行公钥证书的发放，分发和管理。

CA 对主体的公钥签名并发放证书，主要功能有：

1、 证书更新：当前证书过期，发现新证书
2、证书作废：使得该证书从该时刻起非法
3、证书发布：PKI 用户可以搜索并取得证书
4、维护证书作废列表：在 PKI 中保持作废列表的时效
5、发布作废列表：使 PKI 用户可以访问作废列表。

数据传输加密是对传输中的数据流加密，以防止通信线路上的窃听，泄露，篡改和破坏。加密可以在 3 个不同层次来实现，即链路加密，节点加密和端到端加密。链路加密侧重点在通信链路上而不考虑新源何新宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。

端到端加密则指信息由发送端自动加密，进入 TCP/IP 数据包回封，然后作为不可阅读和不可识

别的数据穿过因特网，当这些信息一旦到达目的地，将自动重组，解密成为可读取的数据形式。

实现 VPN 的关键技术主要有隧道技术、加密解密技术、密钥管理技术和身份认证技术。

隧道协议中最为典型的有 IPsec，L2TP，GRE，PPTP，L2F，其中 GRE，IPsec 属于第三层（网络层）隧道协议，L2TP，PPTP，L2F 属于第二层隧道协议。

L2TP 数据吧的封装格式为 IP　UDP　L2TP　PPP

利用报文摘要算法生成报文摘要的目的是防止发送的报文被篡改。

Linux 文件详细信息具体内容详解：

列如：drwxr－ xr－x 2 root root 4096 nov 600:04 aa

第一个字符有 5 种情况：

d ,表示目录文件　　l,表示连接文件

－，表示普通文件　　b,表示设备文件

P,表示普通文件

后面 9 个字符每 3 个一组，分别代表文件所有者，文件所有者所在的用户组，其他用户对文件拥有的权限。rwx 代表读写执行，若没有某权限，用－代替。

“2”表示该目录下的文件数，该文件数目=隐藏文件数+普通文件数

root 代表这个文件（目录）的属主用户为 root

第二个 root 代表这个文件（目录）所属的用户组为 root

4096 代表文件的大小（字节数），目录的大小是 4096 个字节

Nov 6 00:04 是目录修改时间

内存容量问题：

地址编号从 80000H 到 BFFFFH 且按字节编址的

内存容量为(5)KB,若用 16K*4bit 的存储芯

片够成该内存 ，共需(6)片

5.A.128　B.256　C.512　D.1024

6.A.8　　B.16　　C.32　　D.64

解析：

1、80000H 和 BFFFFH 末尾的 H 表示 16 进制

不参与运算。

2、做减法运算（也可都换算成 10 进制）

求出内存容量

BFFFF-80000=3FFFF 10 进制就是 262143B，

然后 262143/1024=256KB，故空（5）答案

是 B、256。

3、算成 bit

256KB=256*1024*8(bit)

16K*4bit=16*1024*4(bit)

4、求出片数

（256*1024*8）/（16*1024*4）=32(片)

故空（6）答案是 C、32。

网络互联基础-TCP/IP 协议族

1、物理层

机械特性：接口的型状，尺寸的大小，引脚的数目和排列方式等。

电气特性：接口规定信号的电压、电流、阻抗、波形、速率及平衡特性等。

功能特性：接口引脚的意义、特性、标准。电压表示范围的含义。

过程特性：确定数据位流的传输方式，事件发生顺序。如：单工、半双工或全双工。

物理层协议有：

美国电子工业协会(EIA)的 RS232，RS422，RS423，RS485 等；际电报电话咨询委员会(CCITT)的 X.25、X.21 等；

物理层的数据单位是位比特(BIT)，典型设备是集线器 HUB。

2、链路层

链路层屏蔽传输介质的物理特征，使数据可靠传送。

内容包括介质访问控制、连接控制、顺序控制、流量控制、差错控制和仲裁协议等。

链路层协议有：

协议有面向字符的通讯协议(PPP)和面向位的通讯协议(HDLC)。

仲裁协议：802.3、802.4、802.5，即：

CSMA/CD(Carrier Sense Multiple Access with Collision Detection)、Token Bus、Token Ring

链路层数据单位是帧，实现对 MAC 地址的访问，典型设备是交换机 Switch。

3、网络层

网络层管理连接方式和路由选择。

连接方式：虚电路(Virtual Circuits)和数据报(Datagram)服务。

虚电路是面向连接的(Connection-Oriented)，数据通讯一次路由，通过会话建立的一条 通路。

数据报是非连接的(Connectionless-Oriented)，每个数据报都有路由能力。

网络层的数据单位是包，使用的是 IP 地址，典型设备是路由器 Router。

这一层可以进行流量控制，但流量控制更多的是使用第二层或第四层。

4、传输层

提供端到端的服务。可以实现流量控制、负载均衡。

传输层信息包含端口、控制字和校验和。

传输层协议主要是 TCP 和 UDP。

传输层位于 OSI 的第四层，这层使用的设备是主机本身。

5、会话层

会话层主要内容是通过会话进行身份验证、会话管理和确定通讯方式。

一旦建立连接，会话层的任务就是管理会话。

6、表示层

表示层主要是解释通讯数据的意义，如代码转换、格式变换等，使不同的终端可以表示。

还包括加密与解密、压缩与解压缩等。

7、应用层

应用层应该是直接面向用户的程序或服务，包括系统程序和用户程序，

例如 www、FTP、DNS、POP3 和 SMTP 等都是应用层服务。

从功能角度可分为三组，1、2 层解决网络信道问题，3、4 层解决传输问题，5、6、7 层处理对应用进程的访问。

从控制角度可分为二组，第 1、2、3 层是通信子网层，第 4、5、6、7 层是主机控制层。

二、TCP/IP 协议簇

TCP/IP 协议簇分为四层，IP 位于协议簇的第二层(对应 OSI 的第三层)，TCP 位于协议簇的第三层(对应 OSI 的第四层)。

TCP 和 IP 是 TCP/IP 协议簇的中间两层，是整个协议簇的核心，起到了承上启下的作用。

1、接口层

TCP/IP 的最低层是接口层，常见的接口层协议有：

Ethernet 802.3、Token Ring 802.5、X.25、Frame reley、HDLC、PPP 等。

2、网络层

网络层包括：IP(Internet Protocol)协议、ICMP(Internet Control Message Protocol)控制报文协议、ARP(Address Resolution Protocol)地址转换协议、RARP(Reverse ARP)反向 地址转换协议。

IP 是网络层的核心，通过路由选择将下一跳 IP 封装后交给接口层。IP 数据报是无连接服务

ICMP 是网络层的补充，可以回送报文。用来检测网络是否通畅。

Ping 命令就是发送 ICMP 的 echo 包，通过回送的 echo relay 进行网络测试。

ARP 是正向地址解析协议，通过已知的 IP，寻找对应主机的 MAC 地址。

RARP 是反向地址解析协议，通过 MAC 地址确定 IP 地址。比如无盘工作站和 DHCP 服务。

3、传输层

传输层协议主要是：传输控制协议 TCP(Transmission Control Protocol)和用户数据报协 议 UDP(User Datagram rotocol)。

TCP 是面向连接的通信协议，通过三次握手建立连接，通讯时完成时要拆除连接，由于 TCP 是面向连接的所以只能用于点对点的通讯。

TCP 提供的是一种可靠的数据流服务，采用“带重传的肯定确认”技术来实现传输的可靠性。

TCP 还采用一种称为“滑动窗口”的方式进行流量控制，所谓窗口实际表示接收能力，用以限制发送方的发送速度。

UDP 是面向无连接的通讯协议，UDP 数据包括目的端口号和源端口号信息，由于通讯不需要连接，所以可以实现广播发送。UDP 通讯时不需要接收方确认，属于不可靠的传输，可能会出丢包现象，实际应用中要求在程序员编程验证。

4、应用层

应用层一般是面向用户的服务。如 FTP、TELNET、DNS、SMTP、POP3。

FTP(File Transmision Protocol)是文件传输协议，一般上传下载用 FTP 服务，数据端口 是 20H，控制端口是 21H。

Telnet 服务是用户远程登录服务，使用 23H 端口，使用明码传送，保密性差、简单方便。DNS(Domain Name Service)是域名解析服务，提供域名到 IP 地址之间的转换。 SMTP(Simple Mail Transfer Protocol)是简单邮件传输协议，用来控制信件的发送、中转。 POP3(Post Office Protocol 3)是邮局协议第 3 版本，用于接收邮件。 数据格式： 数据帧：帧头＋IP 数据包＋帧尾 (帧头包括源和目标主机 MAC 地址及类型,帧尾是校验字)

IP 数据包：IP 头部＋TCP 数据信息 (IP 头包括源和目标主机 IP 地址、类型、生存期等) IP 数据信息：TCP 头部+实际数据 (TCP 头包括源和目标主机端口号、顺序号、确认号、校验字等)