(1)传递需要调制编码。

(1)A.数字数据在数字信道上　　B.数字数据在模拟信道上

C.模拟数据在数字信道上　　D.模拟数据在模拟信道上

【答案】B

【解析】本题考查数字传输与模拟传输和模拟数据和数字数据调制的基本概念。

按承载信息的电信号形式不同，通信可分为模拟传输和数字传输。模拟传输是以模拟信号来传输消息的通信方式，在模拟信道上传输；数字传输是指用数字信号来传送消息的方式，在数字通道上传输。数字数据在数字信道上传输需要将其转变为数字信号，采用相应的数字编码；数字数据在模拟信道上传输需要调制成模拟信号；模拟数据在数字信道上传输时，需要将其通过量化编码转成数字信号；模拟数据在模拟信道上传输时，可以进行调制也可以不进行调制传输。

某一基带系统，若传输的比特数不变，而将二电平传输改为八电平传输，如 T2 和 T8 分别表示二电平和八电平码元间隔，则它们的关系是(2)。

(2)A.T8=3T2　　B.T8=2T2　　C.T8=8T2　　D.T8=4T2

【答案】A

【解析】本题考查数据通信的基本概念。

数据通信系统传输的有效程度可以用码元传输速率和信息传输速率来描述。码元传输速率表示单位时间内数据通信系统所传输的码元个数，这里的码元可以是二进制，也可以是多进制的。信息传输速率又可称为信息速率、比特率等，表示单位时间内数据通信系统所传输的二进制码元个数。在 M 电平传输系统中，信息速率 Rb 和码元率 Rs 之间的关系为：

Rb=Rs log2M

数据通信系统传输中，若传输的比特数不变，传输电平数增加，传输周期就要展宽。本题中，Rb=3Rs，所以 T8=3T2。

偶校验码为 0 时，分组中"1"的个数为(3)。

(3)A.偶数　　B.奇数　　C.未知数　　D.以上都不对

【答案】A

【解析】本题考查数据通信检错和纠错基本知识。

在数据传输过程中，由于信道受到噪声和干扰的影响，可能会出现传输错误，通过在发

送的信息后加冗余位来进行差错控制。寄偶校验码是一种最简单的校验码，其编码规则：先将所要传送的数据码元分组，并在每组的数据后面附加一位冗余位即校验位，使该组包括冗余位在内的数据码元中“1”的个数保持为奇数(奇校验)或偶数(偶校验)。在接收端按照同样的规则检查，如发现不符，说明有错误发生。

用户在开始通信前，必须申请建立一条从发送端到接收端的物理信道，并且在双方通信期间始终占用该信道，这样的交换方式属于(4)。

(4)A.电路交换　　B.报文交换　　C.分组交换　　D.信元交换

【答案】A

【解析】本题考查数据通信的交换方式的概念。

两个终端开始正式通信之前，首先由主呼终端进行呼叫，送出被呼终端的电话号码，直到在主呼和被呼之间建立起一条专用的通信线路，主呼终端和被呼终端才开始进行双向数据传输，在整个数据传输期间一直独占线路，通信结束后释放已建立的通信线路，这种技术叫做电路交换或是线路交换，主要用于电话系统。

发送方待发送的整个数据块称为报文(message)。报文交换事先不建立线路，当发送方有数据块要发送时，它把目的地址附加在报文上交给交换设备，交换设备选择一条合适的空闲输出线，将报文通过该输出线传送出去。在这个过程中，交换设备的输入线和输出线之间不建立物理连接，在每个交换设备处，报文首先被存储起来，在适当的时候被转发出去，所以报文交换采用的是存储转发技术，动态分配线路，使得线路能够共享，提高了资源的利用率。

为了解决报文交换大报文传输的问题，分组交换技术严格限制数据块大小的上限，把大报文切分成更小的数据单位，加上一些必要的控制信息组成的首部后，就构成了分组(packet)，分组从发送端发出，经过一个或多个交换设备转发，转发的选路根据分组的首部信息进行，到达接收端，分组可以在交换设备的内存中缓存，同时保证任何用户都不能独占线路超过几十毫秒，现代网络绝大多数采用分组交换技术。分组交换网由若干个交换机和连接这些交换机的链路组成，每台主机都有一条到交换机的链路，交换机的主要工作就是在它的一条链路上接收输入分组，把这些分组从其他的链路上输出。

信元交换是异步传输模式(Asynchronous Transfer Mode，ATM)采用的交换方式，在很大程度上就是按照虚电路方式进行分组转发。在ATM网络中与众不同的一点是，分组长度是固定不变的，称为信元(cell)。信元长度为53字节，5字节的首部，48字节的有效载荷。

在数字通信中，使收发双方在时间基准上保持一致的技术是(5)。

(5)A.交换技术　　B.同步技术　　C.编码技术　　D.传输技术

【答案】B

【解析】本题考查数据通信的同步方式的概念。

同步控制的方法包括异步起止方式和同步方式。在异步起止方式中，接收方和发送方各自内部有时钟发生器，但频率必须一致。通信双方进行异步串行通信必须遵守异步串行通信控制规程，其特点是通信双方以字符作为数据传输单位，且发送方传送字符的间隔时间是不定的。在同步串行通信方式中，以某种方式将发送方的时钟信号也发送过去，接收方用这个统一的时钟信号来选通数据信号，以此得到和发送完全一致的结果。由于同步串行通信发送端和接收端具有统一的时钟信号，发送和接收的每一位信号都受同步信号的调整，因此，同步串行通信一次传送的信息量比异步串行通信大得多，但是付出的代价是设备复杂。

在OSI参考模型中能实现路由选择、拥塞控制与互连功能的层是(6)。

(6)A.传输层　　B.应用层　　C.网络层　　D.物理层

【答案】C

【解析】本题考查计算机网络的网络体系结构。

计算机网络是一个复杂的系统，通常把计算机网络按照一定的功能与逻辑关系划分成一种层次结构，OSI参考模型是计算机网络的基本体系结构模型，OSI共分为七层，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。

物理层为建立、维持与拆除数据链路实体之间二进制位流传输的物理连接，提供机械的、电气的、功能的和规程的特性。物理连接可以通过中继系统，允许进行全双工或半双工的二进制位流的传输。物理层的数据服务单元是比特，它可以通过同步或异步的方式进行传输。数据链路层是OSI模型的第2层，它介于物理层与网络层之间。用于在相邻结点间建立数据链路，传送以帧为单位的数据，使其能够有效、可靠地进行数据交换。本层通过差错控制、流量控制等，将不可靠的物理传输信道变成无差错的可靠的数据路，将数据组成适合正确传输的帧形式的数据单元，对网络层屏蔽物理层的特性和差异，、使高层协议不必考虑物理传输介质的可靠性问题，而把信道变成无差错的理想信道。

网络层是通信子网的最高层，是高层与低层协议之间的界面层。网络层用于控制通信子网的操作，是通信子网与资源子网的接口。网络层关系到通信子网的运行控制，决定了资源

子网访问通信子网的方式。

设置网络层的主要目的就是为报文分组以最佳路径通过通信子网到达目的主机提供服务，而网络用户不必关心网络的拓扑结构与使用的通信介质。网络层的主要功能如下。

(1)网络连接功能：网络层实体作为数据链路层服务用户，利用各条链路上的数据链路连接服务，来为传送实体之间建立端到端的网络连接关系。其中，涉及到数据通路的建立、维护和拆除的过程。

(2)路由选择功能：路由选择是为建立数据通路服务的一种功能。也就是为在源/宿结点之间建立通路而提供一些控制的过程。这些控制过程由路由算法来实现。

(3)拥塞控制功能：拥塞控制的主要功能是对进入网络的数据流实施有效控制，使通信子网避免发生“网络拥塞”和“死锁”现象，保持稳定运行。

(4)数据传输功能：在网络连接建立之后，网络层实体要为上层递交下来的数据提供传输与中继功能。根据通路的类型，传送服务数据可能在一个子网内进行，也可能要跨越互连设备进行中继转发。传输过程包括对数据的分组、排序以及进行差错和速度控制等。

(5)其他功能：除了具有以上功能外，网络层还提供诸如子网接入、网络连接复用、计费以及在网络互连环境下的协议转换等功能。

传输层是网络体系结构中最关键的一层，是资源子网和通信子网的界面与桥梁，它是面向应用的高层和面向通信的低三层协议之间的接口。传输层主要具有以下功能。

(1)连接管理：传输层连接的管理包括端到端连接的建立、维持和拆除。传输层可同时支持多个进程的连接，即将多个进程连接复用在一个网络层连接上。

(2)优化网络层提供的服务质量:传输层优化网络服务质量包括检查低层未发现的错误、纠正低层检测出来的错误、对接收到的数据包重新排序、提高通信可用带宽、防止无访问权的第三者对传输的数据进行读取或修改等。

(3)提供端到端的透明数据传输：传输层可以弥补低层网络所提供服务的差异，屏蔽低层网络的细节操作，对数据传输的控制包括数据报文分段和重组、端到端差错检测和恢复、顺序控制和流量控制等。

(4)多路复用和分流：当传输层用户进程的信息量较少时，将多个传输连接映射到一个网络连接上，以便充分利用网络连接的传输速率，减少网络连接个数。

应用层功能网络的应用层是网络体系结构中的最高层,它是计算机开放互连环境与本地系统的操作环境和应用系统直接接口的一个层次。在功能上，应用层为本地系统的应用进程(Applicarion Process)访问网络环境提供手段，也是唯一直接给应用;程提供各种应用服务

的层次。即借助应用实体、应用协议和应用服务实现端点用户之间的信息交换。

HDLC 协议采用的帧同步方法为(7)。

(7)A.字节计数法　　B.使用字符填充的首尾定界法

C.使用比特填充的首尾定界法　　D.其他编码法

【答案】C

【解析】本题考查数据链路层协议 HDLC 的基本概念。

数据链路层协议中最有代表性的是高级数据链路控制协议(HDLC)。HDLC 是面向比特的数据链路控制规程，HDLC 协议具有透明传输、可靠性高、传输效率高和灵活性强等特点。HDLC 协议规定了数据传输的操作模式、数据帧格式、帧类型等。

所有的帧都使用下列标准的帧格式，包括链路控制信息和数据。链路控制信息包括帧首和帧尾的标志序列 F、地址字段 A、控制字段 C、帧校验序列 FCS。HDLC 协议规定了长格式和短格式两种帧。长格式包括数据信息字段 I 和链路控制信息，短格式只包含链路控制信息。

HDLC 帧格式

标志序列 F：是一个独特的 8 位序列(01111110)，表示帧的开始和结束。它也可兼作上一个帧的结束标志和下一个帧的开始标志，具有帧同步的作用。标志序列也可用作帧间填充。不包括标志序列在内，如果一个帧的长度小于 32 位，则认为该帧无效。

地址字段 A：在命令帧中，给出执行该命令的次站地址，响应中给出作出应对的次站地址，地址字段通常为 8 位，允许采用扩充地址字段。具体办法是：保留每个 8 位地址的最低位为 0 来表示后面跟着的 8 位是该基本地址的扩充地址，扩充地址的格式与基本地址相同，依次采用上述方法可以多次对地址字段进行扩充。

控制字段 C：用于表示所使用帧的类型以及序列号。该字段也可以被用来去命令被选站执行某种操作，或传递被选站对主站命令的应答。

信息字段 I：表示链路所要传输的实际信息。

帧校验序列 FCS：可以使用 16 位或 32 位的帧校验序列，用于差错检测。

下列哪个协议是无线局域网通信协议(8)。

(8)A.IEEE 1394　　B.IEEE 802.1X　　C.IEEE 802.11　　D.IEEE 802.13

【答案】C

【解析】本题考查有关局域网标准的基本概念。

1980 年 2 月 IEEE 成立 IEEE 802 委员会，负责制定局域网标准`IEEE802 委员会制定一系列标准，主要包括：

IEEE 802.1A：局域网概述及体系结构。

IEEE 802.1B：寻址、网络互连与网络管理。

IEEE 802.2：逻辑链路控制(LLC)。

IEEE 802.3：以太网的 CSMA/CD 总线访问控制方法与物理层规范。

IEEE 802.4：令牌总线(Token Bus)访问控制方法与物理层规范。

IEEE 802.5：令牌环访问控制方法与物理层规范。

IEEE 802.6：城域网(MAN)访问控制方法与物理层规范。

IEEE 802.7：宽带局域网访问控制方法与物理层规范。

IEEE 802.8：FDDI 访问控制方法与物理层规范。

IEEE 802.9：综合语音和数据的访问方法和物理层规范。

IEEE 802.10：网络安全与加密访问方法和物理层规范。

IEEE 802.11：无线局域网访问控制方法与物理层规范。

IEEE 802.12：100VG-AnyLAN 快速局域网访问控制方法与物理层规范。

IEEE 802.14：利用有线电视(Cable-TV)的宽带通信标准。

IEEE 802.15：无线个人区域网(WPAN)规范。

IEEE 802.16：宽带无线网标准。

其中 802.4，802.5，802.12 已经淘汰。

以太网中使用什么机制来检测冲突(9)。

(9)A.CDMA/CD　　B.令牌　　C.CSMA/CD　　D.探测报文

【答案】C

【解析】本题考查局域网的访问控制方式的相关知识。

环型局域网利用环接口设备将传输介质连接成环状，计算机连接到环接口设备上。所组成的环可以是单环，也可以是双环。令牌传递访问控制方式应用在环型局域网上。

以太网的核心技术是共享总线的介质访问控制方法(CSMA/CD)，用于解决多个结点共享总线的发送权问题。

载波侦听多路访问/冲突检测(CSMA/CD)控制方式原理如下：

①每个结点在发送数据前，先监听信道，以确定介质上是否有其他结点发送的信号在传送。

②若介质忙(有信号在传送)，则继续监听。

③否则，若介质处于空闲状态，则立即发送信息。

④在发送过程进行冲突检测。如果发生冲突，则立即停止发送，并向总线上发出一串阻塞信号(全1)强化冲突，以保证总线上所有结点都知道冲突已发生，转⑤。

⑤随机延迟一段时间后返回①。

A、D两个选项与局域网的访问控制方式无关。

一个标准的C类网络(IPv4网络)最多可以划分(10)个子网。

(10)A.128　　B.256　　C.32　　D.64

【答案】D

【解析】本题考查IPv4地址分类和子网划分的有关知识。

1.IP地址

在Internet上的每一台主机和路由器都分配有一个唯一的32位地址，即IP地址，也称作网际地址。IP地址一般采用国际上通行的点分十进制表示。

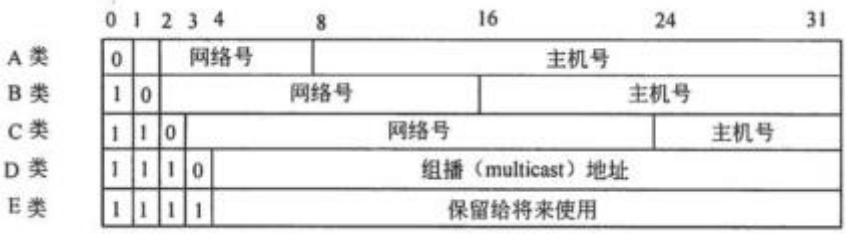
一个IP地址由4个字节组成，字节之间用点分隔，每个字节表示为从0～255的十进制数(8位二进制数最大为11111111，即十进制数255)，这个表示法称为IP地址的点分十进制表示法(dotted decimal notation)。

IP地址由两部分组成：网络号和主机号。网络号标识主机所连接的网络，也叫网络地址：主机号则标识该网络上某个特定的主机，也称主机地址。对一个互联网来说，网络号必须在互联网中唯一，而主机号在该网络内也必须唯一。

一般来说，互联网上的每个接口必须有一个唯一的IP地址，因而多接口主机具有多个IP地址，其中每个接口都对应一个IP地址。

2.IP地址分类

IP协议规定了IP地址分为五类，分别是A、B、C、D、E类。如下图所示。



IP 地址分类是根据网络号的最高几位来区分，图中的格式规定了用作网络号和主机号的位数，因此也就确定了各类地址的网络总数以及每个网络中主机总数。A、B、

C 三类地址可以使用大小不同的网络。

A 类地址的最高位为“0”，其后 7 位是网络号，24 位用作主机号。A 类地址共 126 个网，它用于少数主机数量众多的大型网络，主机数可以 16777216-2=16777214。B 类地址的最高 2 位为“10”，其后 14 位为网络号，16 位用作主机号。B 类地址共 16384 个网，它用于中等规模的网络，每个网络主机数最多为 65536-2=65534。C 类地址的最高 3 位为“110”，其后 21 位为网络号，8 位用作主机号。C 类地址共 2097152 个网，它用于小型网络，每个网络的主机数只能少于 256-2=254。

D 类地址为组播(multicast)地址，它用一个地址代表一组主机。

E 类是实验性地址，保留给将来使用。

在同一个互联网上，IP 地址必须唯一。另外，它还有如下规则：

•A 类地址中以 127 打头的保留作为内部回送地址(loopback)，不能用作公共网地址；

•各比特全 0 和全 1 的网络号和主机号不允许用于分配，用于特殊作用。主机号各比特位全为 0 表示“本地主机”；主机号各位全 1 是代表本网络内所有主机，即网内广播地址，其余的主机号才允许用于分配给网内各主机；网络号为 0 解释为“本网”，网络号全 1 指有限广播网络。

3.子网和子网划分

A 类网络是很大的一个网络，事实上也没有这样大的网络，因此在实际应用中，IP 地址还可以分层：将一个网络分为多个子网，如可将一个 A 类网络分成 256 个 B 类大小的子网(subnet)，同样，B 类地址、C 类地址也可以分层。在分层时，不再把 IP 地址看成由单纯的一个网络号和一个主机号组成，而是把主机号再分成一个子网号和一个主机号。这就是所谓的子网编址(subnet addressing)，现在所有的主机都要求支持子网编址。例如一个 B 类网，可以把主机地址中前 8 位用来表示子网地址，后 8 位留作主机地址，这种 B 类网 IP 地址格式如图下图所示。这样就允许有 254 个子网，每个子网可以有 254 台主机。

0	8	16	24 31
10	网络号	子网地址	主机地址

同一网络中的不同子网用子网掩码来划分，子网掩码(subnet mask)是网际地址中对应网络标识编码的各位 1，对应主机标识编码的各位为 0 的一个四字节整数，也叫做子网屏蔽码。对于 A、B、C 三类网络来说，它们都有自己默认的掩码，即没有划分子网时的掩码，如下图所示。

屏蔽码示例

类	默认的屏蔽码	高 6 位用做子网地址的屏蔽码
A	255.0.0.0	255.252.0.0
B	255.255.0.0	255.255.252.0.0
C	255.255.255.0	255.255.255.252

子网掩码的作用是：如果两台主机的 IP 地址和子网掩码的“与”的结果相同，则这两台主机是在同一个子网中。

4.总结

一个标准的 C 类网络有 8 位(8bit)主机 ID,一个最小的子网至少需要 4 个地址(主机 ID 全 0 和全 1 的地址不能用于分配，剩余两个为主机号)，因此，一个标准的 C 类网络最多可划分 28÷4=64 个子网。

一个 IP 数据包经过一台路由器转发到另一个网络,该 IP 数据包的头部字段中一定会发生变化的是(11)。

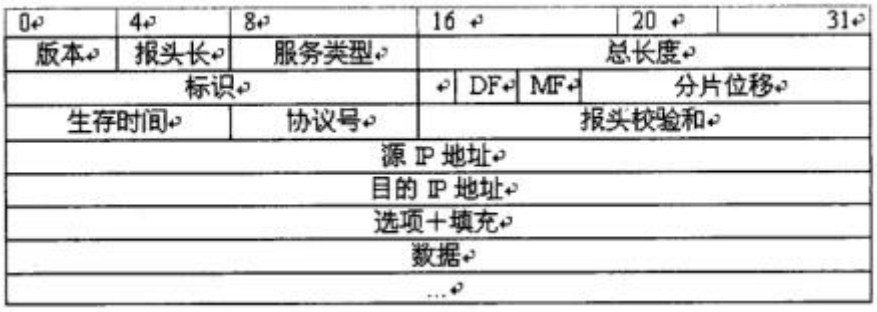
(11)A.源 IP　　B.协议号　　C.目的 IP　　D.TTL

【答案】D

【解析】本题考查路由器的工作原理和 IP 分组中 TTL 字段的含义。

1.IP 数据包结构

IP 数据包是 Internet 的基本传送单元，包括数据包包头和数据区两部分。下图表示了 IP 数据包格式。



IP 数据包格式

IP 协议的数据包头中主要字段如下：

•版本字段

4bit。用来标识 IP 协议的版本。目前的 IP 协议版本是 4，下一代 IP(IPv6)协议为 6。

•包头长度字段

4bito 该字段紧跟在版本号字段后，表示以 32 位(4 个字节)为单位的包头长度。

•服务类型字段

8bit。指明服务类型或优先级，用于实现区分服务或优先级选路机制。

•总长度字段

16bit。以字节为单位的 IP 包长度(包含 IP 头在内)，IP 包最大长度 65535 字节。

•标识符与分段偏移量字段

DP 包可能会被分段，这些字段用于分段和到达目的地后的重组。

•协议字段

协议字段指出用于 IP 数据包携带的高层协议。IP 协议的高层最常用的是 TCP 和 UDP；TCP 的协议代码为 6;UDP 协议代码为 17。

•源地址和目的地址字段

源地址字段和目的地址字段都是 32 位(32bit)。源地址字段存放发送该 IPv4 数据包的原始 IPv4 地址(数据包会经路由器转发，转发路由器地址不是源地址)；目的地址字段存放最终接收该 IPv4 数据包的设备的 IP 地址(转发路由器也会接收其他路由器转发过来的 IPv4 包，但目的地址并不指向该转发路由器)。

2.路由器转发原理

从 OSI 七层模型的角度看，路由器是工作在三层(网络层)，完成三层协议转发的设备。对 Internet 来说，其三层协议就是 IP 协议，因此 Internet 的路由器可以称为 IP 路由器。在 Internet 中，路由器用于连接多个逻辑上分开的网络，这些逻辑网络是指一个单独的网

络或一个子网，用网络 ID 来标识。当数据从一个子网传输到另一个子网时，必须通过路由器转发来完成。路由器具有判断网络地址和选择路径(路由选择)的功能。

总体而言，Internet 路由器是连接 IP 子网的设备，并在两个或多个不同的 IP 子网之间进行 IP 包的转发。IP 子网由 IP 地址中网络 ID(包括子网 ED)部分来标识，网络 ID 不同即为不同的 IP 子网。

3.TTL 字段的作用

TTL 是 Time To Live 的缩写，含义为“生存时间”。为避免因错误选路而产生的环路现象(IP 包在一个循环的路由中传递，永远到达不了目的地)。该字段定义了 IP 数据包可存在的最大期限。由于确切的生存时间很难把握，该字段通常用跳跃站点数来度量，即当数据包从一个网络传送到另一个网络时(即经过一个路由器的转发)，该字段的值减
1。当该字段为 0 时，数据包将被丢弃。

假定在一个 IPv4 网络中只有两个主机 HA 和 HB，HA 和 HB 在同一个 LAN 内，并且没有划分 VLAN。如果 HA 和 HB 需要直接通信则需满足(12)。

(12)A.HA 和 HB 必须在同一子网内

B.HA 和 HB 必须在不同子网内

C.HA 和 HB 无论在一个子网或不在一个子网都可以

D.HA 和 HB 必须使用相同的操作系统

【答案】A

【解析】本题考查 LAN、VLAN 的概念、IP 子网与物理网络的映射关系以及 IP 选路原理。

LAN 是物理上的一个广播域，在 LAN 的所有设备都能收到其他设备的广播信息。VLAN 是逻辑上的广播域，可以把一个 LAN 划分为多个 VLAN。划分 VLAN 后，LAN 内的设备以 VLAN 为单位组成广播域。

在 IPv4 网络中，一个 IP 子网只能映射一个 LAN 或 VLAN;多个 IPv4 子网，可以映射到一个 LAN 或 VLAN 中。

同一子网内主机可直接通信；不同子网之间，主机必须通过路由器才能进行通信。

假定一个 IPv4 网络由 4 段不同的 LAN 互联而成，每段 LAN 上的最大 MTU 值分别是 512、1024、2048 和 4096，则在这个 IPv4 网络上可能出现 IPv4 分组(IP Packet)的最大长度是(13)。

(13)A.512 B.1024 C.2048 D.4096

【答案】D

【解析】本题考查 IPv4 网络中 MTU 的概念和应用。

IPv4 网络中，IPv4 分组(即数据包)的理论最大长度为 65535 字节(参考试题 11 分析中的 IPv4 数据包格式)。但实际应用时，IPv4 分组的长度受制于底层(二层协议)可传送的最大数据长度。MTU(最大传输单元)是指 IP 协议底层(二层)能够传输的最大数据单元长度，单位为字节。

每个 LAN 网段上的 IPv4 子网的底层(二层)网络技术可能是不同的，因此 MTU 的数值也不相同。在每个 LAN 网段上能够传输的最大 IPv4 分组(即数据包)等同于本 LAN 网段的 MTU。如果四个 LAN 网段能够彼此了解相互的 MTU 值，则最大 IPv4 分组长度为 MTU 值的最小值;如果四个 LAN 网段彼此由于某种原因而不能相互了解，则 IPv4 分组的最大长度有可能是最大的 MTU 值(每个 LAN 网段上的 IPv4 分组最大长度分别等于各 LAN 网段上的 MTU 值)。

IPv4 分组长度大于本 LAN 网段内的 MTU 值时，IPv4 分组将进行分段和重组。

一个稳定的 RIP 网络中的一个路由器需要通告 20 条路由，这些路由需要通过一个 UDP 报文来传送。如果这个 UDP 报文每 30 分钟丢失一次，那么对网络路由的影响是(14)。

(14)A.对路由器有影响　　B.对网络有影响

C.对路由器和网络都没有影响　　D.对路由器和网络都有影响

【答案】C

【解析】本题考查 RIP 协议的工作原理，重点考查广播周期和老化周期。

1.RIP 协议

RIP 协议有两个版本：RIP1 和 RIP2。RIP 协议中使用 32 位的因特网地址。路由表中的每一项，可以表示一个主机、一个网络或一个子网。RIP 协议中，路由器需要自己分析路由信息中的地址是代表网络还是主机(参阅 IP 地址分类和子网掩码原理部分)。RIP 协议支持“默认路由”的路由选择方法，默认路由以“0.0.0.0”在路由表中来表示本区域以外的网络路径。

在缺省状态下，RIP 使用非常简单的度量制式(路由表中的开销)：距离是通往目的站点所需经过的链路数——即“跳数”,是取值在 1-15 之间的整数;数值 16 表示无穷大的距离(防止“计数到无穷大”现象)。

RIP 对点到点连接和广播型网络(如以太网)都提供支持。RIP 分组使用 UDP 协议传输。RIP 进程使用 UDP 端口 520 来进行发送和接收。在 RIP 网络中，分组以广播的形式进行发送，

所有与之相连的路由器都会接收该分组。

RIP 分组的定时广播周期是 30s，每个 RIP 网络中的路由器都按该周期定时发送自己的路由表信息(距离向量广播)。RIP 中，路由信息的有效时间是有限制的，规定为 180s，如果 180s 时间内该路由信息未被刷新，则相应的距离被设定为无穷大，该路由记录会从路由表中删除。注意，由于 RIP 网络中，路由器每隔 30s 广播一次自己的路由表信息，因此路由器的路由记录会不断地被刷新(路由记录数据可能不会变化,但收到相同的路由信息即为刷新)。

2.RIP1 和 RIP2

RIP1 是 RIP 的第一个版本，在广播 RIP 路由信息时，RIP 分组中只包含两个主要的数据项：目的(主机或网络)和到达目的的距离。RIP1 不能支持 AS，不能以子网选择路由。为了适应因特网的发展，开发了第二代 RIP 协议 RIP2。

RIP2 是 RIP1 的改进版，主要增加了以下功能：

•支持以子网选择路由(支持子网掩码)。

•支持与 AS 互通(支持 AS 间路由)。

•支持验证机制和多点广播功能。

3.结论

一个稳定的 RIP 网络即为网络拓扑结构不再变化,路由表稳定,此时 RIP 分组 30s 广播一次，路由老化周期为 180s。如果每 30 分钟丢失一次路由器广播 UDP 报文，则不会对路由器和网络产生任何影响。

在一个子网中有一个主机 HA 和路由器 RX，HB 是其他子网的主机。在主机 HA 中到 HB 的路由是 RX(HA 经 RX 到达 HB)。假定在 HA 和 RX 的子网中再增加一个路由器 RY，想让 HA 经 RY 到达 HB，此时需要(15).

(15)A.RY 发送路由重定向 ICMP 报文给 HA　　B.RX 发送路由重定向 ICMP 报文给 HA

C.RY 发送路由重定向 ICMP 报文给 HB　　D.RX 发送路由重定向 ICMP 报文给 HB

【答案】B

【解析】本题重点考查 ICMP 协议中路由重定向的概念。

Internet 网络中的设备可分为路由器和主机两种，在路由器和主机中都需要具有正确的路由表网络才能正常的工作。

在 Internet 中，路由信息的传输分为两种：一种是路由器和主机之间的路由信息传递，它是由 ICMP 的路由功能完成的；另一种是路由器和路由器之间路由信息的交换，它们要依

靠特殊的协议来完成，这些特殊的协议就是路由协议。无论 ICMP 协议还是路由协议，最终要在各自的结点上(包括主机和路由器)维护一个正确的路由表，以路由表决定如何发送(针对主机)和转发(针对路由器)IP 分组。

ICMP 的路由功能包括两个功能：一是发现本地路由器；二是路由重定向。下图显示了 ICMP 报文的路由器广告报文格式(类型=9)。

类型 = 9	代码 = 空	校验和
地址总数	地址表项大小	有效时间
路由器地址 〔1〕		
优先选择级别 〔1〕		
路由器地址 〔2〕		
优先选择级别 〔2〕		

路由器广告报文包含路由器地址列表以及优先级选择级别。ICMP 报文给出了类型值为 9，代码字段为空，表中地址总数和每个表项的大小以及路由器声明的“有效时间”。

发布路由器广告通常目的地址为 224.0.0.1(ICMP 报文在 IP 报文中发送，使用 D 类的组播地址)，该地址代表一个 IP 网络(路由器在哪个网络上广告就代表哪个网络)上的所有主机。如果网络不支持组播地址 224.0.0.1，则使用有限广播地址 255.255.255.255。路由器一般每隔 7min 广播一次路由器广告。路由器广告的有效时间一般是 30min。

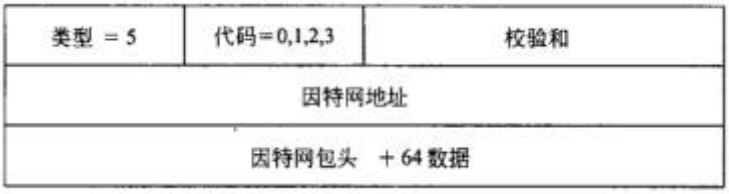
如果主机刚开始工作时，得不到网络上的路由器地址，它可以发送路由器请求报文，其格式如下图所示。

类型 = 10	代码 = 空	校验和
保留		

路由器请求报文目的地址是 224.0.0.2，它代表一个 IP 网络上的所有路由器。收到该请求报文的路由器，可以直接给请求主机发送响应报文(实际上是路由器广告报文)或广播路由器广告报文。

主机收到具有多个路由器地址和优先级的路由器广告后，通过比较网络地址(由子网掩码确定)，忽略不属于本网络的路由器地址。在属于本网络的路由器地址中，挑选优先级最高的路由器地址作为主机的默认路由器。当主机的 IP 分组到达本网络以外的 IP 网络时，如果没有明确的路径到达目的地，则主机的 IP 分组都通过默认路由器进行转发。

默认路由是网络运行的一种好的方法。但有时会增加新的路径。这时需要使用 ICMP 的路由重定向功能。路由重定向报文格式如下图所示：



路由重定向功能可以让本地主机从默认路由器得到到达目的地更好的路径。过程如下：

•主机正常发送分组给默认路由器；

•默认路由器发现有到达目的地更好的路径；

•默认路由器发送路由重定向报文给主机，重定向报文中含有最佳路径的路由器地址；

•主机在本机路由表中增加达到该目的地的新路径。

在 DNS 中，域名是倒树状结构。树根称之为“根域”，根域下面是“顶级域名”。顶级域名中有个“arpa”的顶级域名，其作用是(16)。

(16)A.ARPAnet 组织的简称，是 ARPA 组织的域名

B.ARPA 国家的简称，是 ARPA 国家的域名

C.用作反向地址解析

D.一个普通的顶级域名

【答案】C

【解析】本题考查对 arpa 域名的理解。

DNS 一般是用来通过域名来解析 IP 地址的域名服务系统。DNS 也可以用来做反向解析，即通过 IP 地址得到域名。反向解析使用的域名为 in-addr.arpa。

建立 TCP 连接时需要三次握手，而关闭 TCP 连接一般需要 4 次握手。由于某种原因，TCP 可能会出现半关闭连接和半打开连接这两种情况，这两种情况的描述是(17)。

(17)A.半关闭连接和半打开连接概念相同，是同一现象的两种说法

B.半关闭连接是一端已经接收了一个 FIN，另一端正在等待数据或 FIN 的连接；半打开连接是一端崩溃而另一端还不知道的情况

C.半打开连接是一端已经接收了一个 FIN，另一端正在等待数据或 FIN 的连接；半关闭连接是一端崩溃而另一端还不知道的情况

D.半关闭连接是一端已经接收了一个 FIN，另一端正在等待数据或 FIN 的连接；半打开连接是一端已经发送了 SYN，另一端正在等待 ACK 的连接

【答案】B

【解析】本题考查对 TCP 连接的建立过程和 TCP 连接的关闭过程的理解。

1.TCP 连接的建立

TCP 协议是面向连接的协议，提供可靠的、全双工的、面向字节流的、端到端的服务。TCP 连接是在无连接的 IP 协议上建立的。

TCP 连接建立：TCP 的连接建立过程又称为 TCP 三次握手。首先发送方主机向接收方主机发起一个建立连接的同步(SYN)请求；接收方主机在收到这个请求后向发送方主机回复一个同步/确认(SYN/ACK)应答；发送方主机收到此包后再向接收方主机发送一个确认(ACK)，此时 TCP 连接成功建立。

2.TCP 建立连接过程

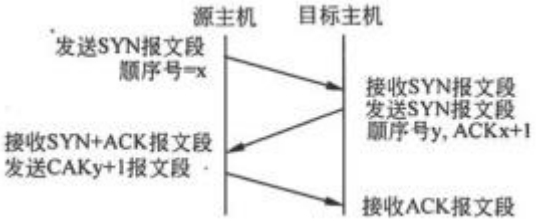
TCP 会话通过三次握手来初始化。三次握手的目标是使数据段的发送和接收 g 步。同时也向对方主机表明其一次可接收的数据量(窗口大小)，并建立逻辑连接。这三次握手的过程可以简述如下：

•源主机发送一个同步标志位(SYN)置 1 的 TCP 数据段。此段中同时标明初始序号(Initial Sequence Number，ISN)。ISN 是一个随时间变化的随机值。

•目标主机发回确认数据段，此段中的同步标志位(SYN)同样被置 1，且确认标志位(ACK)也置 1，同时在确认序号字段表明目标主机期待收到源主机下一个数据段的序号(即表明前一个数据段已收到并且没有错误 k 此外，此段中还包含目标主机的段初始序号。

•源主机再回送一个数据段，同样带有递增的发送序号和确认序号。

至此为止，TCP 会话的三次握手完成。接下来，源主机和目标主机可以互相收发数据。整个过程如下图所示。



TCP 建立连接的三次握手过程

3.TCP 释放连接过程

建立一个连接需要三次握手，而终止一个连接要经过四次握手。这由 TCP 的半关闭

(half-close)造成的。既然一个 TCP 连接是全双工(即数据在两个方向上能同时传递)，因此每个方向必须单独地进行关闭。

TCP 连接的释放需要进行四次握手，步骤是：

•源主机发送一个释放连接标志位(FIN)为 1 的数据段发出结束会话请求。

•目的主机收到一个 FIN，它必须通知应用层对端已经终止了那个方向的数据传送，同时向源主机发回一个确认，并将应答信号(ACK)设置为收到序号加 1，这样就终止了这个方向的传输。

•目的主机此时依然可以向源主机发送数据，数据发送结束后，目的主机也发出一个 FIN 置 1 的报文，请求终止本方向的连接。

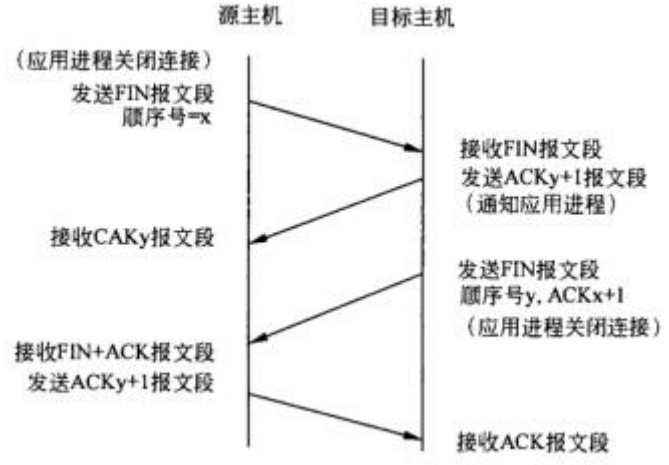
•源主机收到 FIN，再回送一个数据段，带有递增的确认序号。

TCP 释放连接的四次握手过程

4.半打开连接和半关闭连接的概念

TCP 连接经三次握手建立后，如果一方已经关闭或异常终止连接而另一方却还不知道，我们称这样的 TCP 连接为半打开(half-open)连接。任何一端的主机异常都可能导致发生这种情况。只要不打算在半打开连接上传输数据，仍处于连接状态的一方就不会检测另一方已经出现异常。TCP 的 Keepalive 定时器用于发现并结束半打开连接。

TCP 连接建立后，TCP 提供了双向的数据通路。TCP 提供了其中一端结束它的发送后还能接收来自另一端数据的能力，这称为半关闭。半关闭是 TCP 连接关闭过程中完成了前半部分的状态，这时只关闭了一个方向上的数据通道，另一个方向上仍然能够继续数据传输。



IPv6 与 IPv4 相比，下列叙述正确的是(18)。

(18)A. IPv6 地址也分为 A、B、C、D、E 五类

B. IPv6 网络可直接使用 IPv4 的路由协议

C. IPv6 不能实现地址自动配置

D. IPv6 分组的头中增加了流标签(Flow Label)字段

【答案】D

【解析】本题考查对 IPv6(与 IPv4 相比)变化的理解。

IPv6 地址分类与 IPv4 不同，不再分为 A、B、C、D、E 五类；IPv6 中的路由协议不能直接使用 IPv4 的路由协议；IPv6 中可以实现链路本地地址的自动配置；IPv6 的分组头中增加了流标签字段。

IPv6 分组(即数据包)格式如下图所示：

图中的流标号即流标签字段，英文原文为 Flow Label。

一个单位内部的 LAN 中包含了对外提供服务的服务器(WEB 服务器、邮件服务器、FTP 服务器)；对内服务的数据库服务器、特殊服务器(不访问外网)；以及内部个人电脑。其 NAT 原则是：(19)。

(19)A. 对外服务器作静态 NAT；个人电脑作动态 NAT 或 PAT；内部服务器不作 NAT

B. 所有的设备都作动态 NAT 或 PAT

C. 所有设备都作静态 NAT

D. 对外服务器作静态 NAT；内部服务器作动态 NAT；个人电脑作 PAT

【答案】A

【解析】本题考查 NAT 的概念；静态 NAT 和动态 NAT 的应用原则。

IPv4 地址资源有限，面临无地址分配的问题。如何解决呢？方法主要有两个：

方法一：当然是高效利用 IP 地址资源。如减少浪费，把大网如一个 A 类网络，分为子网来进行分配。子网的应用现在已经非常普遍。

方法二：在 Internet 中定义了专用地址空间(RFC1918)如下：

•1 个 A 类地址：10.0.0.0～10.255.255.255

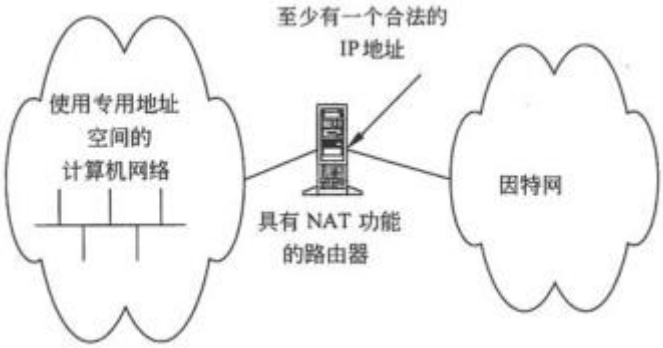
•16 个 B 类地址：172.16.0.0～172.31.255.255

•256 个 C 类地址：192.168.0.0～192.168.255.255

这些地址称为私用地址或专用地址，用户不需要向任何人申请，就可以直接使用；

但是这些地址不允许出现在公共的 Inemet 上。那么用户要访问公共的 Internet 怎么办呢？这要用到地址翻译 NAT(Network Address Translate)技术。

NAT 应用的典型场景如下所示。



这里完成 NAT 功能的路由器或其他设备必须有一个合法的公共 Internet 地址(简称公网 IP 地址)。当私网用户需要访问公网时，通过(私网 IP 地址，端口号)与(公网 IP 地址，端口号)的转换进行访问。

目前的地址转换方式主要有三种，分别是 NAT、PAT 和 Proxy。

NAT：提供一个公网的 IP 地址池，私网用户需要访问公网时，进行公网 IP 地址和私网 IP 地址的映射。

PAT：只提供一个公网的 IP 地址，私网用户需访问公网时，多个私网地址对应一个公网 IP 地址，通过附加端口号来识别。

Proxy：工作在应用层，由代理软件完成数据包的地址转换。

目前，NAT一词可以代表 NAT 和 PAT 的统称，即包含一对一映射和多对一映射。NAT 在实现时又可分为静态 NAT 和动态 NAT。

静态 NAT：一个(私网 IP 地址，端口号)对应一个(公网 IP 地址，端口号)，映射关系由人工指定保持静态不变。主要应用于专网或内部网络上对外提供服务的设备。

动态 NAT：一个(私网 IP 地址，端口号)对应一个(公网 IP 地址，端口号)，但映射关系是动态的，由 NAT 设备根据运行情况随机确定。主要应用于专网或内部网络上的普通用户访问公网时的场景。

下面对电子邮件业务描述正确的是(20)。

(20)A.所有使用电子邮件的设备接收和发送都使用 SMTP 协议

B.必需将电子邮件下载到本地计算机才能察看、修改、删除等

C.须使用专用的电子邮件客户端(例如 Out Look)来访问邮件

D.电子邮件体系结构中包含用户代理、邮件服务器、消息传输代理和邮件协议

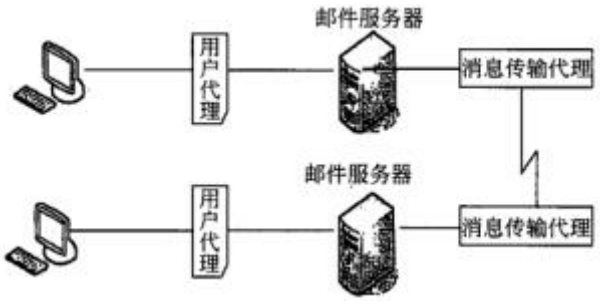
【答案】D

【解析】本题主要考查电子邮件(E-mail)系统的组成和所使用的协议。

1.电子邮件体系结构

电子邮件服务是因特网基本的服务之一，是一种因特网上使用最广泛的服务。它提供一种快速、简便的信息传输手段。电子邮件系统是以电子信息传输手段传输以电子信息形式存储的邮件的系统。所谓电子邮件，就是以电子信息形式存储的信件。我们发送、接收邮件时是以电子手段进行处理的。

一个电子邮件体系结构中包含用户代理、邮件服务器、消息传输代理和邮件协议。如下图所示。



2.POP3、SMTP 协议及服务器

一般邮件客户与邮件服务器之间需要某种协议以存取用户在邮件服务器上的邮件或发送邮件到邮件服务器。在这两个方向上，邮件客户和邮件服务器之间使用的协议是不同的。SMTP 英文是 Simple Mail Transfer Protocol，意为简单邮件传输协议。是计算机之间传输

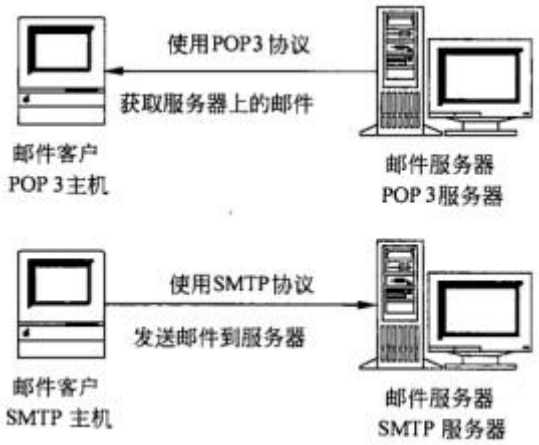
电子邮件的协议。该协议主要规定基础的电子邮件提交系统怎么传递报文，即电子邮件怎么通过两个计算机之间的物理链路，从一个计算机传输到另一个计算机。SMTP 非常简单，它没有规定电子邮件系统怎样从用户接收邮件等。用户从邮件服务器上接收邮件要使用 POP3 协议。

POP 英文是 Post Office Protocol，意为邮局协议，POP3 是这个协议的版本 3。它使邮件客户可以用一种比较实用的方法来访问存储于服务器上的邮件。通常，这意味着邮件客户可以从服务器上取得邮件，而服务器为它暂时保存邮件。

下图中表明了这两种服务器的作用。邮件客户在发送和接收时，使用的是不同功能的服务器。这两个服务器可以由一个计算机完成，也可以是两个不同的计算机。

3.IMAP4 协议

IMAP revl(RFC2060)是 Internet Message Access Protocol 的缩写，是通过 Internet 获取信息的一种协议。IMAP4 是 IMAP 协议的第 4 个版本，正如 POP3 是 POP 协议的第 3 个版本一样。IMAP 是一种强有力的邮箱访问方式。



POP3 提供了快捷的邮件下载服务，用户可以利用 POP3 把邮箱里的信下载到 PC 上进行离线阅读。一旦邮件进入 PC 的本地硬盘，就可以选择把邮件从服务器上删除，然后脱离与 Internet 的连接并选择在任何时候阅读已经下载的邮件。

IMAP 支持用户在线阅读功能，支持 Web Mail 功能(不下载到本地，所有邮件都在邮件服务器上)，允许用户在服务器上建立任意层次结构的文件夹，并且可以灵活地在文件夹之间移动邮件，随心所欲地组织你的邮箱。当然，IMAP 也支持邮件下载到本地阅读(等同 POP3 功能)

在互联网上，当我们访问一个设备时，(21)。

(21)A.必须要有域名，才能访问　　B.有 IP 地址就可以访问

C.必须同时有 IP 地址和域名　　D.必须要有域名服务器

【答案】B

【解析】本题主要考查对 IP 地址和域名作用的理解。

在 Internet 上通信，需要 IP 地址即可进行。域名系统是为了便于人们记忆需要的互联网(Internet)服务而产生的。

比如，通过浏览器访问新浪网 www.sina.com.cn，系统首先通过 DNS 系统查找到该域名对应的 IP 地址(正向解析)，然后把用户信息封装为 IP 分组(数据包)进行传输和通信。

对于一个稳定的 OSPF 网络(单区域)，下面描述正确的是(22)。

(22)A.必需指定路由器的 Router ID，所有路由器的链路状态数据库都相同

B.无需指定路由器的 Router ID，路由器之间的链路状态数据库可以不同

C.定时 40s 发送 Hello 分组，区域中所有路由器的链路状态数据库都相同

D.定时 40s 发送 Hello 分组，区域中路由器的链路状态数据库可以不同

【答案】A

【解析】本题考查对单区域 OSPF 工作原理的理解。

1.OSPF 概念

OSPF 即开放最短路径优先协议(Open Shortest Path First)，是为了解决距离矢量类路由选择协议存在的问题而开发的。

RIP 协议是最早出现的路由协议，它采用距离矢量路由算法进行路由信息传递，这种协议的中心思想是：定时更新路由表，选择开销最小的路由。距离矢量类选择协议的缺点是收敛速度慢、跳数限制以及容易产生环路等。

OSPF 协议属于链路状态路由选择协议，采用 SPF 算法来计算路由表。OSPF 协议的核心思想是：网络中的每个路由器都有一个相同的唯一的网络图(链路状态数据库)，通过 SPF 算法，每个路由器独立计算出自己的路由表。这里每个路由器有两张表：“网络图”即链路状态数据库(LSDB)和路由表。OSPF 协议的主要功能是维护“网络图”的一致性和正确性，如果网络发生了变化，把变化传递给每个路由器，保证新的“网络图”反映最新的网络拓扑结构；同时每个独立的路由器根据最新的“网络图”，通过 SPF 算法，得到新的路由表。

2.关键术语 ’

•链路：所谓链路就是在网络中两个路由器间的物理的或逻辑的连接，链路状态包括传

输速度、延迟、接口类型等一些属性。 -

•网络图：即链路状态数据库(LSDB)。OSPF 网络中，所有连接路由器的逻辑的或物理的链路信息的总和。实际上就是网络的拓扑结构组成图。

•路由器标识符(Router ID):用于标识每个路由器的 32 位数。通常，一个路由器有多个接口(Interface)，包括物理接口和虚拟接口(loopback)，每个接口都会分配 IP 地址，那么如何标识这个路由器呢？原则是：使用所有接口中 IP 地址最大 IP 数值来标识该路由器，称为 RouterlD。如果在路由器上使用了 loopback 接口，优先选择 loopback 的最高 IP 地址。

3.Hello 协议和扩散协议

OSPF 由两个互相关联的主要部分组成：Hello 协议和扩散(Reliable Flooding)机制。Hello 协议用于检测邻居是否可达；Hello 协议操作在每个活跃的 OSPF 接口上，它使用的组播地址使得这些流量不会对非 OSPF 的路由器造成影响。扩散算法确保 OSPF 区域中所有路由器具有完全一致的链接状态数据库。

OSPF 协议支持在广播型网络(如以太网)、点到点网络和非广播型网络(NBMA 网络，如 FR、ATM 等)上的运行。其 Hello 协议的参数选择如下：

OSPF 环境	Hello 间隔	Down 机判定间隔
广播	10 秒	40 秒
点对点	10 秒	40 秒
NBMA	30 秒	120 秒

以广播型网络(以太网)为例，每 10 秒发送一个 Hello 包，如果 40 秒内收不到邻居发送的 Hello 包，则判断邻居不可达。

4.结论

一个稳定的 OSPF 单区域网络，网络的拓扑结构稳定，即 LSDB 中的链路不发生变化，此时所有的路由器中的 LSDB 都相同。

下列对 FTP 业务的描述正确的是(23)。

(23)A.FTP 服务必须通过用户名和口令才能访问。FTP 可以基于 UDP 或 TCP 传输信息

B.FTP 服务器必须通过用户名和口令才能访问。FTP 只能基于 TCP 传输信息

C.FTP 服务器无须用户名和口令即可访问。FTP 可以基于 UDP 或 TCP 传输信息

D.FTP 服务器无须用户名和口令即可访问。FTP 只能基于 UDP 传输信息

【答案】B

【解析】本题考查对数据业务的理解和对 FTP 业务的访问机制的理解。

FTP 业务属于文件传输类的数据业务。针对 Internet 网络而言，文件传输要保证可靠性(文件传输不能有差错)，对实时性要求不高(可以有大的延迟或延迟抖动)。因此 FTP 业务是基于 TCP 协议而实现的。

FTP 在用户下载时需要提供用户名的口令；即使是匿名登录，其实本质上也是有用户名(anonymous)和口令(任意邮箱格式 xxx@xx.xxx)。

下列对集成服务(IntServ)模型和区分服务(DiffServ)模型描述正确的是(24)。

(24)A.IP 的 QoS 技术主要是集成服务模型和区分服务模型

B.集成服务模型和区分服务模型无法进行结合

C.集成服务扩展性好，可以应用在不同规模的网络中；区分服务扩展性差，不能应用在大型网络中

D.集成服务模型可以计对单个业务(比如一路电话)进行 QoS 保证;区分服务模型不针对单个业务，而是针对一类业务进行 QoS 保证

【答案】D

【解析】本题主要考查对集成服务(IntServ)模型和区分服务(DiffServ)模型的理解。

1.IPQoS 技术

在通信和计算机网络中，服务质量简称 QoS。QoS 分广义和狭义之分：狭义的 QoS 指技术指标(传输时延、抖动、丢失率、带宽要求、吞吐量等)；广义的 QoS 指资源调配与利用、层与层之间的协商，从而涉及不同层次的 QoS。

QoS 在 IETF 中的定义为“A set of service requirements to be met by the network while transporting a flow”，即网络在传输数据流时要满足的一系列服务要求，具体可量化为狭义的 QoS 技术指标。

Internet 最初是面向非实时的、数据类型通信而设计的。IP 协议提供无连接的、不可靠的、尽力而为的网络层服务。传统的 IP 传输服务被称为尽力而为的服务(Best Effort Service)。

尽力而为类型的服务无法满足对实时性要求较高的业务(如电话、视频业务等)的要求，于是 IETF 提出借鉴 QoS 技术，加强实现资源的控制和调度机制，使得网络能够支持各种类型的业务;为此 IETF 提出了综合服务模型(Interagted Servicearchitecture,简称 IntServ，中文也翻译为综合服务体系)和分类业务模型(Differentiated Service Achitecture，简称

DiffServ，中文也翻译为区分服务体系)。

2.集成服务(IntServ)模型

IntServ 是根据每个 IP 流 QoS 等级的精确描述，由具有 RSVP 功能的路由器中的 RSVP 协议和流的接纳控制支持 IP 的 QoS 分类。集成服务模型可以针对单个业务(由流来标识)进行端到端的 QoS 保证服务。

在 IntServ 流中，定义了三类业务 保证业务(Guaranteed Service，GS)、受控负载业务(Controlled Load Service，CLS)和尽力而为的服务(Best Effort Service，BES)。对于 GS 业务，流的最大排队时延是受到控制的，路由上的任何时延都会影响最大排队时延。而 CLS 没有固定的时延保证，但业务流要与在网络轻载情况下的流质量相当，实际上 CLS 要求有长期的带宽保证。总之，这两种业务都要求用令牌漏斗协块来定义流的特性，超出的业务流被当作 BES 型业务量处理。BES 业务是传统的 IP 服务提供的 i 务类型。

IntServ 中定义 RSVP 为其 QoS 信令。通过 RSVP，用户可以给每个业务流申请资源预留，要预留的资源可以包括缓冲区及带宽大小。这种预留需要在路径上的每一跳上进行，这样才能提供端到端的 QoS 保证。

利用资源预留可以使路由器能够提前决定是否有能力满足业务的需求，为每个流预留需要的网络资源，并建立相应的策略控制信息，即所谓“软状态”。

“软状态”信息在路由器上等同增加了转发策略，即附加的路由转发策略。这样路由器需要维护的“软状态”信息的数量与业务流的数量是线性关系。因此 IntServ 在具体实现时，其主要缺点就是扩展性较差，在骨干网上，业务流的数量十分庞大，路由器无法完成相应量级的“软状态”处理和资源预留工作。

3.分类业务(DiffServ)模型

IETF 的 DiffServ 模型是基于每跳行为(Per Hop Bahaviors，PHB)的概念，DiffServ PHB 由路由上的每个本地路由器所具有的前转行为来定义。目前，IETF 已定义两种主要的 PHB：

•加速前转 PHB(Expedited Forwarding PHB，EF-PHB)

EF-PHB 的特征是带宽具有可配置性并在同一链路上不受其他业务量的影响。EF-PHB 可以用来在 DiffServ 域中建立要求具有低丢失率、低时延与低时延抖动的端到端业务。

•可确定的前转 PHB 组(Assured Forwarding PHB Group，AF-PHB 组)

AF-PHB 组的特征是有 4 个 AF 等级，每个等级分配有一定量的转发资源(比如在一个 DiffServ 结点上的缓存与带宽等)。在每一个 AF 等级中，各个 IP 分组被标记上三种可能的丢弃优先级。当发生拥塞时，分组的丢弃优先级将决定在某一 AF 等级中各分组的相对重要

性。4 个 AF 等级的相对性能之间没有标准的关系，AF-PHB 组可以实现以较高的可能性保证业务所要求的信息速率。

分类业务模型的核心思想是对业务流进行分类，针对不同种类的业务进行转发。在一个分类域中，所有的路由器都采用同样的转发策略——最终体系在 PHB;在一个分类域的边界进行业务流的分类和标记工作。

分类业余模型可以在 Internet 骨干网上大规模实现，但其不能针对单个业务流进行端到端的 QoS 保证。

4.综合业务模型和分类业务模型的结合

这两种技术可以统合起来形成支持 QoS 敏感(aware)型 IP 业务的网络模型。在 IETF 给出的框架中，端到端的 QoS 是由网络边缘的 IntServ 区域与网络核心的 DiffServ 区域一起提供的，这一方式常被称为“核心边缘”方式。

MPLS 是一种将(25)路由结合起来的集成宽带网络技术。

(25)A.第一层转发和第二层　　B.第二层转发和第三层

C.第三层转发和第四层　　D.第四层转发和第七层

【答案】B

【解析】本题考查对 MPLS 技术核心思想的理解。

MPLS 最初是基于 ATM 技术发展起来的。它结合 ATM 技术和 IP 技术各自的优点。其核心思想是：边缘路由，核心交换。从协议层次上来观察即为：结合了第二层转发和第三层路由的集成宽带网络技术。

在一个局域网上，进行 IPv4 动态地址自动配置的协议是 DHCP 协议。DHCP 协议可以动态配置的信息是(26)。

(26)A.路由信息

B.IP 地址、DHCP 服务器地址、邮件服务器地址

C.IP 地址、子网掩码、域名

D.IP 地址、子网掩码、网关地址(本地路由器地址)、DNS 服务器地址

【答案】D

【解析】本题考查 DHCP 协议的作用。

DHCP 中文翻译为动态主机配置协议，主要为要上网的设备动态配置上网参数。如果一

个设备需要访问互联网，其必备的参数是：IP 地址、子网掩码、网关地址(本地路由器地址)；如果需要用域名访问互联网，则还需要配置 DNS 服务器地址。

BGP 是 AS 之间进行路由信息传播的协议。在通过 BGP 传播路由信息之前，先要建立 BGP 连接，称之为“BGP Session”。下列对 BGP Session 连接描述正确的是(27)。

(27)A.BGP Session 基于 IP 协议建立　　B.BGP Session 基于 UDP 协议建立

C.BGP Session 基于 TCP 协议建立　　D.BGP Session 基于 ICMP 协议建立

【答案】C

【解析】本题考查对 BGP 协议的了解。

边界网关协议(BGP)经历了不同的阶段，从 1989 年的最早版本 BGP1，发展到 1993 年开始开发的最新版本 BGP4。BGP4 支持 CIDR 和超网。

BGP 使用路径矢量路由算法，为了避免 AS 间的路由环路(距离矢量算法的缺点)，AS 采用了路径向量的概念。路径向量是指，在传递到达某目的地(以 CIDR 形式的网络 ID 标识)的路由时，附加此路由经过的 AS 号。这样，当一个 AS 中的边界路由器收到某个路由时，只需要看看路径中是否包含有自己所在 AS 的号码便可判断是否有 AS 间环路。

BGP 是用来在自治系统(AS)之间传递选路信息的路径向量协议。BGP 利用了传输控制协议(Transmission Control Protocol，TCP)提供的可靠传输服务。这消除了 BGP 实现更新数据包的分段、重传、确认和先后顺序问题的需要，因为 TCP 已经完成了这些功能。另外，任何 TCP 使用的认证方法也可以利用于 BGP。

BGP 会话建立成功后，BGP 就使用通常的 Keepalive 消息来维护会话的完整性。Update 消息也可以重置保持计时器(hold timer)，这一计时器的典型值是 keepalive 计时器(keepalive timer)值的 3 倍。如果连续 3 次收不到 Keepalive 消息，也没有 Update 消息，那么 BGP 会话就会被关闭。

P2P 业务和 C/S(或 B/S)结构的业务主要差别是(28)。

(28)A.P2P 业务模型中每个结点的功能都是等价的，结点既是客户机也是服务器

B.P2P 业务模型中的超级结点既是客户机也是服务器，普通结点只作为客户机使用

C.P2P 业务模型与 CS 或 BS 业务模型的主要区别是服务器的能力有差别

D.P2P 业务模型与 CS 和 BS 业务模型的主要区别是客户机的能力有差别

【答案】A

【解析】本题主要考查对 P2P 概念的理解。

C/S 是英文 Client/Server 的缩写，中文翻译为客户/服务器模式。C/S 结构的业务中 Client 和 Server 的功能和作用是不同的。Client 端主要完成业务的请求并处理和呈现返回结果；Server 端主要完成接收 Client 端提出的服务请求、进行相应的处理并将结果返回给 Client 端的功能。

C/S 业务体系结构一般需要开发专用的客户端和服务器端软件，并针对不同的计算机操作系统开发不同的版本。其扩展性、服务升级的方便性、移植性都受到很大限制。

B/S 业务结构是基于 C/S 结构的，它们之间并没有本质的区别。B/S 是基于特定通信协议(HTTP)的 C/S 架构，也就是说 B/S 包含在 C/S 中，是特殊的 C/S 架构。B/S 业务结构中客户端使用通用浏览器软件，Server 端使用基于通用的 Web 服务器的综合服务软件系统。

P2P 是英文 peer-to-peer 的简称，中文翻译为“对等网络”。P2P 是一种网络结构的思想，与目前网络中占据主导地位的 C/S 结构(包括 B/S)的一个本质区别是：整个网络结构中不存在中心结点(或中心服务器)。在 P2P 结构中，每一个结点(peer)大都同时具有信息消费者、信息提供者和信息通讯等三方面的功能。

在 P2P 网络中每一个结点所拥有的权利和义务都是对等的。从功能上说，每个结点(peer)既是客户机又是服务器，既能请求服务，也向其他结点(peer)提供服务。通俗的讲，P2P 可以直接将人们联系起来，让人们通过互联网直接交互。P2P 改变了互联网现在的以服务器为中心的状态、重返“非中心化”，并把权力交还给用户。

用 UTP cat5 作为通信介质，用一层以太网设备互联，最大联网距离是(29)。

(29)A.100m　　B.205m　　C.500m　　D.2500m

【答案】C

【解析】本题主要考查共享式以太网的联网法则。

1.以太网组网和一层组网设备

组建以太网时如果不使用任何网络互连设备，其网络范围是有限的(受限于通信介质)。要扩大以太网的组网范围，可以使用互连设备完成。用于互连以太网的设备可以分为两类：第一层互连设备，称为中继器；第二层互连设备，称为网桥。

中继器从原理上看，是工作在 OSI 协议模型第一层的设备，即工作在物理层。它只对经过它的以太网信号进行放大。中继器的主要作用是把经过该设备的以太网信号进行整形、放大等处理后，以广播方式传送到设备的所有端口，目的是扩大以太网的物理覆盖范围，即连

网的范围。

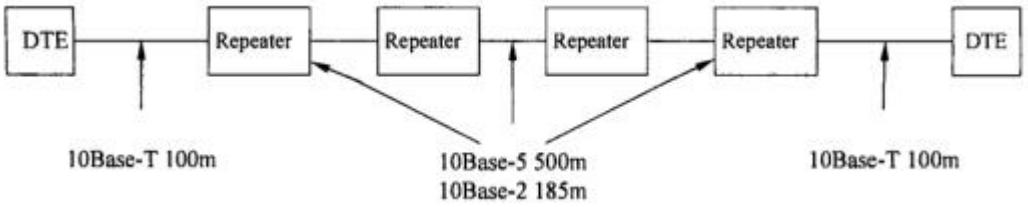
由于中继器设备只是简单的信号放大设备，用中继器互连的以太网，称为一个冲突域。中继器不能隔离以太网中的冲突(它对任何信号均放大广播，包括冲突信号)。

用中继器设备组网，又可称为共享式以太网组网。

2.共享式 10Mbps 以太网组网原则

10Mbps 以太网有三个标准：10Base5、10Base2 和 10Base-T。共享式 10Mpbs 以太网组网原则是：5-4-3-2-1 法则，如下图所示。

5 是指用中继器互连的以太网中,两个结点(图中的 DTE 设备)之间最大可以有 5 个网段；4 是指最大可以有 4 个中继器；3 是有三个网段可以接入 DTE 设备(即计算机结点)；2 是有两个网段作互连网段：1 是指整个连网属于一个冲突域。



3.10Base-T 共享式集线器组网

10Base-T 以太网中 T 表示传输介质是双绞线，所以 10Base-T 又称双绞线以太网。双绞线有两种类型：非屏蔽双绞线 UTP 和屏蔽双绞线 STP。STP 双绞线外围有一层金属网称为屏蔽层，可以屏蔽外界电磁波辐射，抗干扰能力强，传输性能好，但价格高；UTP 由于没有屏蔽层，性能较差，但价格低廉。

目前双绞线以太网连网时一般使用 UTP，UTP 双绞线按其传输性能又分为几种：cat3、cat4、cat5、cat6 或更高，称为 3 类 UTP、4 类 UTP、5 类 UTP，数值越大，表明传输性能越好。UTPcat5，称为 5 类 UTP 双绞线，可以用于 10Mbps、100Mbps、1000Mbps 的以太网组网使用，是目前综合布线应用最广泛的通信介质。

在以上所述任何类型的双绞线中，一根双绞线内部包含 8 根绞合成 4 对的子线。简单讲就是，一根双绞线中有 4 对线。

10Base-T 连网介质使用 3 类或 5 类 UTP 或 STP;连网采用主机一集线器(HUB)模式,双绞线以太网中，共享式集线器就是中继器，应该遵守中继器的连网法则；主机到集线器最大距离为 100m;非特别指明，HUB 隐含是指共享式集线器，即双绞线以太网的中继器；因此共享式 10BASE-T 用一层设备组网，最大距离是 500m。

4.100Mbps 共享式以太网

100Mbps 以太网称为快速以太网，它主要有三个标准规范：

•100Base-T4：4 对线，cat3 或更高。连线范围 100m。

•100Base-TX：2 对线，cat5。连线范围 100m。

•100Base-FX：为纤介质。

如果使用 UTPcat5，其单段连网(不使用连网设备)距离为 100m。使用中继器(共享式 100Mbps 集线器)时，最多允许两个中继器，并且两个中继器之间 UTPcat5 连接长度不超过 5m。即，采用一层设备连网，最大连网范围是 205m。

5.1000Mbps 共享式以太网

如果使用共享式 1000Mbps 以太网(通信介质 UTPcat5)组网，只能使用一个中继器。单段连网(不使用连网设备)距离为 100m。则最大联网距离为 200m。

实际上，1000Mbps 铜线以太网，一般使用超 5 类和 6 类 UTP 作为通信介质。

二层以太网交换机联网范围主要受制于(30)。

(30)A.MAC 地址　　B.CSMA/CD　　C.通信介质　　D.网桥协议

【答案】D

【解析】本题主要考查对二层设备工作原理和网桥协议的理解。

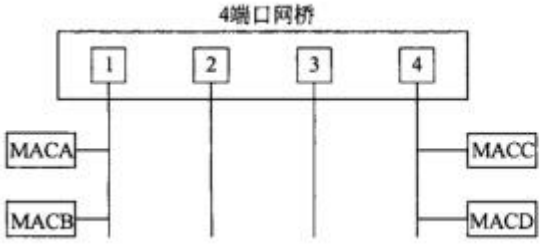
1.网桥(以以太网为例说明)

网桥是工作在 OSI 协议模型第二层的设备。其和中继器的主要区别是，它根据以太网的帧信息进行以太网帧的转发。在以太网中，传输信息是以以太网帧格式进行传输的。在以太网帧中，包含了 DA—标识目的地址和 SA—标识源地址。以太网帧格式如下。

前导 1010..1010	SFD 10101011	DA	SA	长度	LLC 数据	LLC 填充	FCS
56位	8位	6字节	6字节	2字节	46—1500字节		4字节

802.3 数据包帧格式

网桥设备内部有一个转发表，称为网桥的路由表。表中存有以太网地址(简称 MAC 地址)和网桥物理端口的对应。如下图所示。



物理端口号	物理端口上的设备 (以MAC地址标识)
1	MACA，MACB
4	MACC，MACD
2	……
3	……

网桥在物理端口上收到以太网信息后，根据以太网帧中的目的地址，查自己的路由表进行转发。网桥能够区分不同的物理以太网网段，即用中继器互连的以太网。

网桥的转发表是通过自己学习得到的。网桥的每个端口都监听本端口上的所有以太网帧，从监听到的以太网帧的源地址字段得到MAC地址和物理端口的对应关系，并填充自己的转发表。

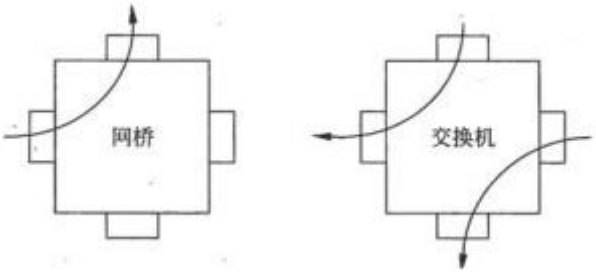
如果有设备同时出现在网桥的两个端口上，则网桥就不能正常工作了，因此用网桥互连的网络不能出现环路。

2.二层交换设备

二层交换设备本质上也是网桥，工作原理相同，但它是一种功能更强，性能更好的网桥。可以实现多个端口之间同时转发以太网帧。

网桥一般采用软件实现以太网帧的转发，转发数据时，同时只能在两个端口之间进行(无论网桥有多少个端口)。

二层交换，一般指用硬件代替软件进行以太网帧的转发，并且同时能够在交换设备的多个端口之间同时进行转发。下图给出了网桥和交换机的转发差别。



3.网桥协议

基于网桥的工作原理，用二层设备互连的网络不能有环路。但在实际连网时，我们希望不同网段之间有链路备份，即同一物理连接，具有两个或两个以上的连接通道。这时环路将大量存在。为了解决设备的环路问题，二层设备上必须运行网桥协议。

网桥协议的核心算法是生成树算法。IEEE(电机和电子工程师学会)制定了802.1D的生成树协议(Spanning Tree Protocol)，它在防止产生环路的基础上提供路径冗余。生成树协议(STP)是通过生成树算法(STA:Spanning Tree Algorithm)计算出一条到根网桥的无环路路径来避免和消除网络中的环路，它是通过判断网络中存在环路的地方并阻断冗余链路来实现这个目的。通过这种方式，它确保到每个目的地都只有唯一路径，不会产生环路，从而达到管理冗余链路的目的。

为了实现对冗余链路的管理，找出存在的冗余链路，STA在网络中选举根网桥作为依据，

跟踪该可用路径。若发现存在冗余路径，它将选择最佳路径来进行数据包转发，并阻断其他冗余链路。

4.网桥协议的问题和连网距离

STA 运行需要二层设备不断交换链路信息(物理连接的信息)，其有信息广播的周期和 STA 算法收敛速度的问题。如果用二层设备组网的规模过大，信息传播和算法收敛将变的不可预测。按经验原则(无理论证明)，一般二层设备组网最大可到 7 级左右(7 个二层设备级联)。

VLAN 实施的前提条件是(31)。

(31)A.使用 CSMA/CD 协议　　B.基于二层设备实现

C.基于二层交换机实现　　D.基于路由器实现

【答案】C

【解析】本题考查 VLAN 的概念和实现基础。

VLAN 是在二层实现的，是基于二层交换设备实现的。在普通的网桥上(非交换式)将无法实现 VLAN。

在以太网半双工共享式连接中，我们无需流量控制；而在全双工交换式连接中要考虑流量控制，其原因是(32)。

(32)A.共享式连接中，由共享式集线器(Hub)完成流量控制

B.共享式连接中，CD(碰撞检测)起到了拥塞避免的控制机制。全双工中必须附加其他机制来完成

C.全双工交换式连接带宽扩大了一倍，必须增加流量控制机制

D.为了在全双工网络中实现 VLAN，必需增加流量控制机制

【答案】B

【解析】本题考查对 CSMA/CD 和全双工的概念的理解。

共享式或半双工以太网采用带有碰撞检测的载波侦听多路访问(CSMA/CD)的方法进行媒体访问控制。按照这种方法，一个工作站在发送前，首先侦听媒体上是否有活动。所谓活动是指媒体上有无数据传输，也就是载波是否存在。如果侦听到有载波存在，工作站便推迟自己的传输。如果侦听的结果为媒体空闲时，则立即开始进行传输。在侦听到媒体忙时，采用一定的延迟后(有不同的回避策略)，可继续检测。如果有两个以上的工作站，同时检测到媒

体空闲，同时发送数据，此时就会产生碰撞；每个工作站，在发送数据的同时，也进行碰撞检测，一旦检测到碰撞，将终止当前数据的发送，延迟一定的时间(随机的时间，以减小下次发生碰撞的概率)，然后再检测并发送。

从CSMA/CD的工作原理看，当用户业务量增大时，碰撞就会增加，此时实际的传输数据量将下降。CSMA/CD原理的核心是竞争使用传输媒体，其机制本身就能进行流量控制。

全双工交换式连接，将CSMA/CD机制中的CD取消，同时保证每个物理连接上只有两个设备(点到点连接)，这样点到点连接的两个设备可以同时进行数据收发操作。由于缺少了碰撞检测，CSMA本身无法控制用户的业务流量，全双工交互式连接必须额外增加流控机制来控制用户的业务流量。

若在一个IPv4网络中一共划分了5个VLAN，则该IPv4网络中(33)。

(33)A.至少存在5个子网　　B.最多存在5个子网

C.至少存在5个路由器　　D.最多存在5个路由器

【答案】A

【解析】本题考查IP子网与VLAN的映射关系以及IP选路原理。请参考试题(12)分析部分。

在IPv4网络中，一个IP子网只能映射一个LAN或VLAN;多个IPv4子网，可以映射到一个LAN或VLAN中。

同一子网内主机可直接通信；不同子网之间，主机必须通过路由器才能进行通信。

有一个IPv4网络，使用172.30.0.0/16网段。现在需要将这个网络划分为55个子网，每个子网最多1000台主机，则子网掩码是(34)。

(34)A.255.255.64.0　　B.255.255.128.0

C.255.255.224.0　　D.255.255.252.0

【答案】D

【解析】本题考查子网划分方法和表示方法。

55个子网，取最接近的2的幂的整数是64，即2的6次方1000个主机，取最接近的2的幂的整数是1024，即2的10次方。

即172.30.0.0/16的最后10bit表示主机ID，其余为网络用子网掩码来表示为255.255.252.0。

应用 MPLS VPN 时，针对每个 VPN 地址规划应满足的条件是(35)。不同的 VPN 信息通过 MPLS 骨干网(或核心网)时通过(36)进行区分。

(35)A.每个 VPN 都是独立的，可以使用任何地址，只要保证在 VPN 内部合法正确即可

B.VPN 之间的地址不能相互重叠

C.VPN 内只能使用公网 IP 地址

D.VPN 内只能使用私网 IP 地址

(36)A.IP 地址+AS 号　　B.IP 地址+子网掩码

C.VPN 标识符　　D.VPN 标识符+IP 地址

【答案】A　　D

【解析】本题考查 VPN 的概念和 MPLS VPN 的工作原理。

1.VPN 的概念

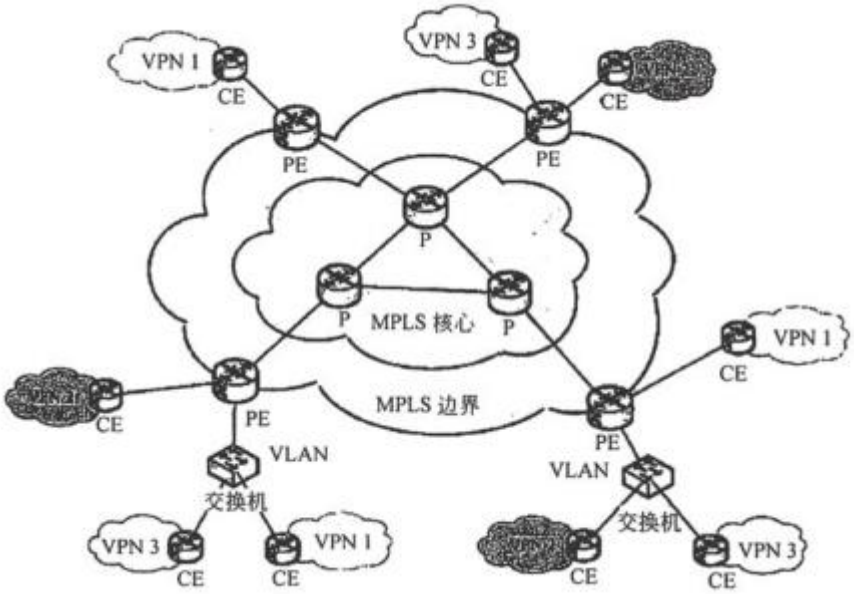
虚拟专用网络(Virtual Private Network，VPN)是建立在公网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而是通过 ISP 提供的公用网络来实现通信，其专用性表现在 VPN 之外的用户无法访问 VPN 内部的资源，VPN 内部用户之间可以实现安全通信。

简单地说，VPN 指在 Internet 上建立的、由用户(组织或个人)自行管理的网络。VPN 的实现是依靠相关技术，在公共的 Internet 上传送专用的、保密的用户私有数据。从用户角度看，VPN 就是自己的专网，只不过，它是通过 VPN 技术在公共的 Internet 网络上虚拟出的网络资源。

2.MPLS VPN

MPLS VPN 可以基于二层或三层实现。《网络规划设计师教程》中提及的 MPLSVPN 属于 MPLS 三层 VPN。

MPLS 三层 VPN 是一种基于 PE 的 L3VPN 技术。它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。MPLS 三层 VPN 的典型结构如下所示。



MPLS 三层 VPN 模型由三部分组成：CE、PE 和 P。

•CE(Customer Edge)：用户网络边缘设备，有接口直接与服务提供商 SP(Service Provider)网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。

•PE(Provider Edge)：服务提供商边缘路由器，是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。

•P(Provider)：服务提供商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。

MPLS 三层 VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE，因此得到越来越多的应用。

3.结论

VPN 是用户的专用网络，因此每个 VPN 是独立的。如果每个 VPN 是独立的，就存在地址重叠问题，即两个或多个 VPN 内部的地址信息是重叠的，此时只传递 VPN 内部的路由信息就无法正常进行选路。

要在存在地址重叠的 MPLS 三层 VPN 的 MPLS 骨干(或称核心)网上正确传递 VPN 路由，就必须传递两个信息：VPN 内部的路由信息(用 IP 地址标识)和 VPN 的标识，其中 VPN 标识用于 PE 之间识别要传递到那些 VPN，IP 地址(包括子网标识)用于传递 VPN 内部的路由信息。

有一个公司内部网络发生了故障，故障现象是：甲用户可以正常使用内部服务器和互联

网服务，乙用户无法使用这些服务。那么检测故障最佳的方法是：(37)。

(37)A.从乙用户所在的物理网络的物理层开始检查故障，依次检测物理层、数据链路层、网络层直到应用层

B.从乙用户所在的物理网络的路由器开始检查故障，依次检测路由器，二层交换机、中继器或 HUB

C.从检测公司的服务器开始，依次检测服务器、网络互联设备、物理层连接

D.从甲用户所在的物理网络首先开始检测，依次检测物理层、数据链路层、网络层直到应用层

【答案】A

【解析】本题考查综合的故障检测能力。

在一个公司内部，有人能访问内部服务器和外部服务器，有人不能访问。此时应判断出应用层(对应各种服务)和网络层(外部网络和公司内部网络的公共部分)很有可能是可靠的；而问题很有可能出现在乙用户自己本身或者乙用户所在的网络区域。因此最佳方法是从乙用户的物理层开始检测，依次为物理层、数据链路层、网络层直至应用层。

某局域网内部有 30 个用户，假定用户只使用 E-mail(收发流量相同)和 Web 两种服务，每个用户平均使用 E-mail 的速率为 1Mbps，使用 WEB 的速率是 0.5Mbps，则按照一般原则，估算本局域网的出流量(从局域网向外流出)是(38)。

(38)A.45Mbps　　B.22.5Mbps　　C.15Mbps　　D.18Mbps

【答案】D

【解析】本题考查对通信流量分布的简单规则的掌握和应用

1.通信流量分布的简单规则

在通信规范分析中，最终的目标是产生通信量，其中必要的工作是分析网络中信息流量的分布问题。在整个过程中，需要依据需求分析的结果来产生单个信息流量的大小，依据通信模式、通信边界的分析，明确不同信息流在网络不同区域、边界的分布，从而获得区域、边界上的总信息流量。

对应部分较为简单的网络，可以不需要进行复杂的通信流量分布分析，仅采用一些简单的方法，例如 80/20 规则、20/80 规则等；但是对于复杂的网络，仍必须进行复杂的通信流量分布分析。

2.80/20 规则

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：在一个网段中，通信流量的 80%是在该网段内流动，只有 20%的通信流量是访问其他网段。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

3.20/80 规则

随着互联网的发展，一些特殊的网络不断产生，例如小区内计算机用户形成的局域网、大型公司用于实现远程协同工作的工作组网络等。这些网络的特征就是：网段的内部用户之间相互访问较少，大多数对网络的访问，都是对网段外的资源进行访问。对应这些流量分布恰好位于另一个极端，可以采用 20/80 规则。

20/80 规则的思路是：根据对用户和应用需求的统计，产生网段内的通信总量大小，其中 20%的通信流量是在该网段内流动，80%的通信流量是访问外部网段。

80/20 规则和 20/80 规则虽然比较简单,但这些规则是建立在大量的工程经验基础上的；另外通过这些规则的应用，可以很快完成一个复杂网络中大多数网段的通信流量分析工作，可以合理减少大型网络中的设计工作量。

4.与具体互联网业务相结合。

E-mail：发送邮件和接收邮件。视为对等流量，即 50%流出，50%流入。

Web：浏览网络，从 web 下载的流量大。使用 20/80 法则。流出：20%，流入 80%。

本题答案：流出流量：30×1×50%+30×0.5×20%=18Mbps。

在采用公开密钥密码体制的数字签名方案中，每个用户有一个私钥，可用它进行(39)；同时每个用户还有一个公钥，可用于(40)。

(39)A.解密和验证　　B.解密和签名　　C.加密和签名　　D.加密和验证

(40)A.解密和验证　　B.解密和签名　　C.加密和签名　　D.加密和验证

【答案】B　　D

【解析】本题考查公开密钥密码体制的基础知识。

与只使用一个密钥的对称传统密码不同，公钥密码学是非对称的，它依赖于一个公开密钥和一个与之在数学函数上相关但不相同的私钥。由于公钥可以对外公开，通常用于加密和签名认证(这样与之通信的多个用户可以共用一个加密密钥，密钥管理开销小)，私钥是用户自己保管的，通常用于解密和签名。

关于防火墙的功能，下列叙述中哪项是错误的？(41)。

(41)A.防火墙可以检查进出内部网络的通信量

B.防火墙可以使用过滤技术在网络层对数据包进行选择

C.防火墙可以阻止来自网络内部的攻击

D.防火墙可以工作在网络层，也可以工作在应用层

【答案】C

【解析】本题考查防火墙的基础知识。

在建筑上，防火墙被设计用来防止火势从建筑物的一部分蔓延到另一部分，而网络防火墙的功能与此类用于防止外部网络的损坏波及到内部网络。其基本工作原理是在可信任网络的边界(即常说的在内部网络和外部网络之间，通常认为内部网络是可信任的和安全的，而外部网络是不可信的和不安全的)建立起访问控制系统，隔离内部和外部网络，执行访问控制策略，防止外部的未授权结点访问内部网络和非法向外传递内部信息。防火墙一般安放在被保护网络的边界，只有在所有进出被保护网络的通信都通过防火墙的情况下，防火墙才能起到安全防护作用。

如果针对内部网络的攻击是来自网络内部的话，其相关通信数据不会经过防火墙，则防火墙的访问控制安全策略不能对攻击通信数据加以检查和控制，所以防火墙不能阻止来自网络内部的攻击。也就是说防火墙只能防“外贼”不能防“内贼”。

以下哪种技术不是实现防火墙的主流技术?(42)。

(42)A.包过滤技术　　B.NAT 技术　　C.代理服务器技术　　D.应用级网关技术

【答案】B

【解析】本题考查实现防火墙主要技术的基础知识。

防火墙技术可根据防范的方式和侧重点的不同分为：包过滤型技术、应用级网关技术、代理服务器技术三种类型。

NAT(Network Address Translation，网络地址转换)是一种将私有(保留)地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。NAT 技术在解决 IP 地址不足的同时，能隐藏并保护网络内部的计算机，从而能有效地避免来自网络外部的攻击，通常同防火墙技术配合使用。但是它本身不是实现防火墙的技术。

PKI 的基本组件不包括以下哪个部分？(43)。

(43)A.注册机构 RA　　B.认证机构 CA　　C.证书库　　D.公开可访问的目录

【答案】D

【解析】本题考查 PKI(Public Key Infrastructure，公钥基础设施)的系统组成的基础知识。

PKI 是一个采用公钥理论和技术来提供安全服务的具有普适性的安全基础设施，是网络安全建设的基础及核心。PKI 采用证书来进行公钥管理，其主要目的是通过自动管理密钥和证书，为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而有效地保护通信数据的机密性、完整性和有效性。

一个典型的 PKI 系统框架通常包括注册机构 RA、认证机构 CA 和证书发布系统。其中认证机构 CA 负责管理公钥的整个生命周期，其作用包括发放证书、规定证书的有效期和发布证书废除列表；注册机构 RA 提供用户和 CA 之间的一个接口，主要完成收集用户信息和确认用户身份的功能；证书发布系统负责证书的集中存放，用户可以从此处获得其他用户的证书和公钥，一般采用证书库或目录服务。“公开可访问的目录”有迷惑的效果，但是并不等同于目录服务。

以下哪项功能电子签名(electronic signature)不能提供：(44)。

(44)A.电子文件的保密性　　B.电子文件的完整性

C.能鉴别文件签署者的身份　　D.文件签署者同意电子文件的内容

【答案】A

【解析】本题考查电子签名技术的基础知识。

电子签名具有法律效用。从技术的角度，电子签名以电子形式存在，依附于电子文件并与其逻辑关联，可用以识别电子文件签署者身份，保证文件在传输过程中没有受到破坏(即保证电子文件的完整性)，并表示签署者同意电子文件的内容。

保密性和完整性不是同一个概念，保密性要求信息不被泄露给未授权的人，完整性要求信息会受到各种原因的破坏。电子文件的保密性通常需要由加密技术来提供。电子签名技术和加密技术是相互独立的，虽然两者经常结合起来使用。

企业主页上的内容是提供企业的相关消息供大家访问，这时不需要保护消息的(45)。

(45)A.可靠性　　B.完整性　　C.保密性　　D.真实性

【答案】C

【解析】本题考查网络安全的基础知识。

保密性是指信息泄露给非授权用户/实体/过程从而被非法利用；完整性指未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失；可靠性指系统能正常工作不出故障；真实性指信息的来源是真实的或身份是真实的。

企业主页上的内容是公开给所有人看的，也就是说所有人都是合法授权用户，因此不需要采用措施来保证保密性。

小王在安装基于 UNIX 的服务器系统时想给系统增加安全审计功能，最简便的做法是(46)。

(46)A.启动和配置 UNIX 操作系统的各种系统日志功能

B.安装 NetSC 日志审计系统

C.安装防火墙

D.安装入侵检测系统

【答案】A

【解析】本题考查安全审计的基础知识。

安全审计包括识别、记录、存储、分析与安全相关行为的信息。对于计算机系统，这些信息通常保持在系统日志中。因此如果想增加 UNIX 的服务器系统的安全审计功能，只需启动和配置 UNIX 操作系统的各种系统日志功能，就能在系统日志中保存同审计相关的数据。

关于加密技术，下面哪种说法是错误的？(47)。

(47)A.为提高安全性，密码体制中加密算法和解密算法应该保密

B.所有的密钥都有生存周期

C.密码分析的目的就是千方百计地寻找密钥或明文

D.公开密钥密码体制能有效地降低网络通信中密钥使用的数量

【答案】A

【解析】本题考查密码体制的基础知识。

对于一个好的密码体制,其安全强度应该不依赖于密码体制本身(包括明文的统计特性、加密操作方式、处理方法和加/解密算法、密钥空间及其统计特性等)的保密，而只依赖于密钥。

某公司的人员流动比较频繁，网络信息系统管理员为了减少频繁的授权变动，其访问控制模型应该采用(48)。

(48)A.自主型访问控制　　B.强制型访问控制

C.基于角色的访问控制　　D.基于任务的访问控制

【答案】C

【解析】本题考查访问控制技术的基础知识。

访问控制是指主体依据某些控制策略或权限对客体本身或是资源进行的不同授权访问。访问控制包括三个要素：主体、客体和控制策略。访问控制模型是一种从访问控制的角度出发，描述安全系统，建立安全模型的方法。访问控制模型通常分为自主型访问控制模型、强制型访问控制模型、基于角色的访问控制模型、基于任务的访问控制模型和基于对象的访问控制模型。

自主型访问控制模型的特点是授权的实施主体自主负责赋予和回收其他主体对客体资源的访问权限;强制型访问控制模型的特点是系统对访问主体和受控对象实施强制访问控制，主体和客体都被分配了一个固定安全属性，根据主体/客体的安全属性决定主体是否能够访问客体;基于角色的访问控制模型的特点是访问控制由各个用户在部门中所担任的角色来确定，而不是基于员工在哪个组或谁是信息的所有者；基于任务的访问控制模型的特点是以从任务(活动)的角度来建立安全模型和实现安全机制,在任务处理的过程中提供动态实时的安全管理。

本题中给出的条件是公司的人员流动比较频繁,但是公司中的角色(职位)一般是不会变化，因此适合采用基于角色的访问控制模型。

用 IPSec 机制实现 VPN 时，如果企业内部网使用了私用 IP 地址，应该采用(49)技术，IPSec 该采用(50)模式。

(49)A.NAT 技术　　B.加密技术　　C.消息鉴别技术　　D.数字签名技术

(50)A.传输模式　　B.隧道模式

C.传输和隧道混合模式　　D.传输和隧道嵌套模式

【答案】A　B

【解析】本题考查 VPN 和 IPSec 的基础知识。

VPN 的目标是在不安全的公共网络上建立一个安全的专用通信网络，通常采用加密和认

证技术，利用公共通信网络设施的一部分来发送专用信息，为相互通信的结点建立起的一个相对封闭的、逻辑上的专用网络。构建 VPN 需要采用“隧道”技术，建立点对点的连接，使数据包在公共网络上的专用隧道内传输。

在 IPSec 协议中有两种工作模式：传输模式和隧道模式。这两种模式的区别非常直观——它们保护的对象不同，传输模式保护的是 IP 载荷，而隧道模式保护的是整个 IP 包。由于企业内部网使用了私用 IP 地址，必须通过 NAT 转换为公网地址才能与外界通信。同时由于是搭建 VPN，IPSec 应该工作在隧道模式才能建立起 VPN 所需的隧道。

关于入侵检测系统的描述，下列叙述中哪项是错误的？(51)。

(51)A.监视分析用户及系统活动　　B.发现并阻止一些已知的攻击活动

C.检测违反安全策略的行为　　D.识别已知进攻模式并报警

【答案】B

【解析】本题考查入侵检测系统的基础知识。

入侵检测系统是通过从计算机网络和系统的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定的措施的系统。

入侵检测系统的目标在检测和发现攻击活动，自身并不能阻止攻击活动。只有与防火墙等设备联动，才有可能阻止一些攻击活动。

AH 协议中用于数据源鉴别的鉴别数据(ICV)是由 IP 分组中的校验范围内的所有“固定”数据进行计算得到的，以下哪个数据不在计算之列？(52)。

(52)A.IP 分组头中的源 IP 地址　　B.IP 分组头中的目的 IP 地址

C.IP 分组头中的头校验和　　D.IP 分组中的高层数据

【答案】C

【解析】本题考查 IPSec 协议中的 AH 协议的基础知识。

AH 协议中用于数据源鉴别的鉴别数据(ICV)是由 IP 分组中的校验范围内的所有“固定”数据进行计算得到的，也就是说原 IP 数据包头中不变的或接受端可预测的字段都会在安全保护范围之内，如果在传输过程中发生改变，则 ICV 也会发生改变。

4 个选项中“IP 分组头中的头校验和”选项会随着其他一些可变字段(如存活时间 TTL 等)的变化而变化，不属于固定数据，故不在计算之列。

特洛伊木马程序分为客户端(也称为控制端)和服务器端(也称为被控制端)两部分，当用户访问了带有木马的网页后，木马的(53)部分就下载到用户所在的计算机上，并自动运行。

(53)A.客户端　　B.服务器端　　C.客户端和服务器端　　D.没有

【答案】B

【解析】本题考查特洛伊木马程序的基础知识。

对木马程序而言，它一般包括两个部分：客户端(控制端)和服务器端(被控制端)。服务器端安装在被控制的计算机中，一般通过电子邮件或其他手段让用户在其计算机中运行，以达到控制该用户计算机的目的。客户端程序是控制者所使用的，用于对受控的计算机进行控制。服务器端程序和客户端程序建立起连接就可以实现对远程计算机的控制。

以下哪种程序不属于恶意代码？(54)。

(54)A.widget　　B.特洛伊木马　　C.僵尸程序　　D.网络蠕虫

【答案】A

【解析】本题考查恶意代码的基础知识。

恶意代码指未经用户授权而干扰或破坏计算机系统/网络的程序或代码。恶意代码通常具有如下共同特征：具有恶意的目的；自身是计算机程序；通过执行发生作用。一般分为特洛伊木马、僵尸程序、网络蠕虫、计算机病毒、间谍软件和垃圾邮件等。

widget 指能够面向最终用户独立运行的功能实体，一般来讲根据运行位置的不同可以分为 Web Widget、桌面 Widget 和移动 Widget 等，它的表现形式可能是视频，地图，新闻，小游戏等等，Widget 是当前非常流行的一项技术，能够极大地方便用户的桌面应用和网络应用。它的根本思想来源于代码复用，不具有恶意的目的。

黑客小张一天想尝试入侵某公司网络，窃取机密信息。为提高效率，他需要做的第一步工作通常是(55)；第二步通常是(56)；在成功入侵该公司网络某台主机并取得该主机的控制权后，通常所作的工作是(57)；在窃取到机密信息后，最后需要做的工作是(58)；为了预防黑客入侵的第一步，该公司网络应该采取的预防措施为(59)；针对第二步的预防措施为(60)。为了能及时发现上述入侵，该公司网络需要配备(61)。

(55)A.收集目标网络的所在位置及流量信息

B.到网上去下载常用的一些攻击软件

C.捕获跳板主机，利用跳板主机准备入侵

D.通过端口扫描等软件收集目标网站的 IP 地址、开放端口和安装的软件版本等信息

(56)A.了解目标网络的所在位置的周围情况及流量规律，选择流量小的时间发起攻击

B.下载攻击软件，直接发起攻击

C.向目标网络发起拒绝服务攻击

D.根据收集的开放端口和安装的软件版本等信息，到网络查找相关的系统漏洞，下载相应的攻击工具软件

(57)A.修改该主机的 root 或管理员口令，方便后续登录

B.在该主机上安装木马或后门程序，方便后续登录

C.在该主机上启动远程桌面程序，方便后续登录

D.在该主机上安装网络蠕虫程序以便入侵公司网络中的其他主机

(58)A.尽快把机密数据发送出去

B.在主机中留一份机密信息的副本，以后方便时来取

C.删除主机系统中的相关日志信息，以免被管理员发现

D.删除新建用户，尽快退出，以免被管理员发现

(59)A.尽量保密公司网络的所在位置和流量信息

B.尽量减少公司网络对外的网络接口

C.尽量关闭主机系统上不需要的服务和端口

D.尽量降低公司网络对外的网络接口速率

(60)A.安装网络防病毒软件，防止病毒和木马的入侵

B.及时对网络内部的主机系统进行安全扫描并修补相关的系统漏洞

C.加大公司网络对外的网络接口速率

D.在公司网络中增加防火墙设备

(61)A.入侵检测系统　　B.VPN 系统　　C.安全扫描系统　　D.防火墙系统

【答案】D　D　B　C　C　B　A

【解析】本题考查黑客攻击及防御的基础知识。

黑客攻击的典型攻击步骤如下：1)信息收集，信息收集在攻击过程中的位置很重要，直接影响到后续攻击的实施，通常通过扫描软件等工具获取被攻击目标的 IP 地址、开放端口和安装的软件版本等信息；2)根据收集到的相关信息，去查找对应的攻击工具；3)利用查找

到的攻击工具获得攻击目标的控制权；4)在被攻破的机器中安装后门程序，方便后续使用；5)继续渗透网络，直至获取机密数据；6)消灭踪迹，消除所有入侵脚印，以免被管理员发觉。针对上述的攻击过程，需要尽量关闭主机系统上不需要的服务和端口防止黑客收集到相关信息，同时需要及时对网络内部的主机系统进行安全扫描并修补相关的系统漏洞以抵御相应攻击工具的攻击。为了能及时发现上述入侵，需要在关键位置部署 IDS。

网络安全应用协议 SSL 协议工作在(62)，HTTPS 协议工作在(63)。

(62)A.数据链路层　　B.网络层　　C.传输层　　D.应用层

(63)A.数据链路层　　B.网络层　　C.传输层　　D.应用层

【答案】C　D

【解析】本题考查网络安全应用协议的基础知识。

SSL(Secure Sockets Layer 安全套接层)的设计目标是在 TCP 基础上提供一种可靠的端到端的安全服务，其服务对象一般是 Web 应用。它指定了一种在应用层协议和 TCP/IP 协议之间提供数据安全性分层的机制，因此它工作在传输层。这个协议的第三版 SSLv3 经过改进后被 IETF 的 TLS 工作组接受作为传输层安全协议(Transport Layer Security，TLS)。HTTPS(Hypertext Transfer Protocolover Secure Socket Layer，基于 SSL 协议的 HTTP)，提供了身份验证与加密通信方法，用于安全的 HTTP 数据传输，因此它工作在应用层。

在实施网络规划项目时，创建项目工作分解结构的作用是(64)。

(64)A.协调项目利益相关者的要求

B.确认项目经理并进行授权

C.分析项目涉及的工作，明确项目任务范围

D.监测项目的成本执行情况以衡量项目绩效

【答案】C

【解析】本题考查项目范围管理方法“工作分解结构(WBS)”的基本知识。

工作分解结构是一种以结果为导向的分析方法，用于分析项目所涉及的工作，所有这些工作构成了项目的整体范围。工作分解结构是计划和管理项目进度、成本和变更的基础，是项目管理中一个非常基本的文件。因此，创建项目工作分解结构的作用是分析项目涉及的工作，明确项目任务范围。

在对项目中某项活动所耗费的时间进行估算时，可给出三个时间估计：乐观时间 to、悲观时间 tp、最可能时间 tm，则该项活动的期望工期为(65)。

(65)A. $\frac{t_o+t_m+t_p}{3}$ B. $\frac{t_o+2t_m+t_p}{4}$ C. $\frac{t_o+3t_m+t_p}{5}$ D. $\frac{t_o+4t_m+t_p}{6}$

【答案】D

【解析】本题考查项目管理中活动历时估计方法的基本知识。

在对项目中要完成的各项活动的历时进行估计时，当存在高度不确定因素时，可采用概率时间估计法，对活动确定三个估计时间，即：乐观时间 to、最可能时间 tm 和悲观时间 tp。采用三个时间估计时，是假定三个估计均服从 3 概率分布，在这个假定的基础上，活动的期望工期可以用公式 $\frac{t_o+4t_m+t_p}{6}$ 计算。

在项目成本管理中，估算完成项目所需资源总成本的方法不包括(66)。

(66)A.类比法 B.甘特图法 C.参数模型法 D.自下而上累加法

【答案】B

【解析】本题考查项目管理中成本估算方法的基本知识。

项目的成本估算需要给出完成项目所需资源成本的近似值。成本估算的主要技术包括：类比估算法、自下而上估算法和参数模型估算法。类比估算法是使用以前相似项目的实际成本作为目前项目成本估算的根据；参数模型法是应用项目特征参数建立数学模型来估算成本；自下而上累加法是在工作分解结构的基础上，分别估算每个工作包的成本，然后自下而上将所有的估算相加，最终完成整个项目的估算。而甘特图法是进行项目进度管理的最常用的工具，其通常形式是纵向表示项目的各项工作，横向表示所需的时间，不具备成本估算的功能。

根据《中华人民共和国著作权法》和《计算机软件保护条例》的规定，对于法人或其他组织的软件著作权，保护期为(67)。

(67)A.20 年 B.30 年 C.50 年 D.70 年

【答案】C

【解析】本题考查软件相关知识产权保护法规的基础知识。

《计算机软件保护条例》规定：软件著作权属于软件开发者，软件著作权自软件开发完成之日起产生。自然人的软件著作权，保护期为自然人终生及其死亡后 50 年，法人或者其

他组织的软件著作权，保护期为50年。

项目每个阶段结束时的一个重要工作是进行项目绩效评审，评审的主要目标是(68)。

(68)A.决定项目是否能够进入下一个阶段

B.根据过去的绩效调整项目进度和成本基准

C.评定员工业绩和能力

D.得到客户对项目绩效认同

【答案】A

【解析】本题考查项目管理中有关项目生命周期管理的基础知识。

由于项目具有一定的不确定性，将一个项目划分为若干阶段，是有效实施管理与控制的常用做法。例如，可将项目生命周期划分为项目定义、项目开发、项目实施、项目收尾四个阶段。对于每个阶段应明确工作目标和任务，在每个阶段结束时，要对该阶段的绩效进行评审，检验阶段目标达成情况，及时发现和解决其中存在的问题，避免将问题带入下一个阶段，只有通过了阶段绩效评审，项目才能够进行下一个阶段。

在对规划项目进行经济效益评价时，常使用净现值、净现值率、投资回收期、内部收益率等评价指标。当(69)时，规划项目具有经济可行性。

(69)A.净现值大于0　　B.投资回收期大于行业基准投资回收期

C.内部收益率小于行业的基准收益率　　D.折现率大于行业基准收益率

【答案】A

【解析】本题考查项目经济效益评价主要指标的含义和评价标准。

净现值是指按行业基准收益率或设定的折现率，将项目计算期内各年净现金流量折现到建设期初的现值之和。该指标表示项目在整个寿命期内所取得的净收益的现值，如果净现值大于0，说明项目能够盈利、具有经济可行性；如果净现值小于0，说明项目不具有经济可行性。

净现值率是项目净现值与项目总投资现值之比，常用于多方案比较，能够反映资金的利用效率。

投资回收期是指以项目的净收益抵偿全部投资所需要的时间。投资回收期越短说明项目盈利能力越强。在项目评价中，要将计算出的项目投资回收期与行业的基准投资回收期进行比较，前者小于后者时，表明项目能在规定的时间内收回投资，否则项目不具备经济可行性。

内部收益率是指项目在整个计算期内各年净现金流量现值累计等于零时的折现率，它反映了项目以每年的净收益归还全额投资以后，所能获得的最大收益率。只有当内部收益率大于行业的基准收益率时，项目才具备经济可行性。

折现率本身并不是评价指标，而是用于计算净现值、动态投资回收期等指标的参数，可预先设定，或取定为行业基准收益率。

某企业拟建设通信网络对外提供服务。根据市场预测，未来业务发展好的概率为0.7，业务发展差的概率为0.3。现有三种规划方案可供选择：

方案1，直接投资3000万元大规模建网。若业务发展得好，每年可获利1000万元，若业务发展不好，每年亏损200万元，服务期为10年；

方案2，投资1400万元建设小规模网络。若业务发展得好，每年可获利400万元，若业务发展不好，每年仍可获利300万元，服务期为10年；

方案3，前3年按方案2实施，即先投资1400万元建设小规模网络，收益同方案2。3年后若业务发展不好，则继续按方案2实施；若业务发展得好，则再追加投资2000万元进行网络扩容，扩容后服务期为7年，每年可获利950万元。

根据以上条件经计算可知(70)。

(70)A.方案1的期望净收益为5000万元　　B.方案3的期望净收益为3595万元

C.方案1为最优方案　　D.方案2为最优方案

【答案】B

【解析】本题考查风险型决策方法和概率相关的基础知识。

在风险型决策问题中，各种方案的实施在不同的条件下所导致的后果是不一样的，而各种条件和后果出现的概率是可以测算的，决策者可以通过计算出各方案在不同条件下的期望收益来考虑未来的经济效果。针对本题分别计算三种方案的期望净收益，期望净收益最大的为最优方案。

该方案1的期望净收益为：

[0.7×1000+0.3×(-200)]×10-3000=3400(万元)。

方案2的期望净收益为：

(0.7×400+0.3×300)×10-1400=2300(万元)。

方案3的期望净收益为：

0.7×(400×3-2000+950*7)+0.3×300×10-1400=3595(万元)。

计算结果表明，方案3的期望净收益最大，因此，方案3为最优方案。

A glue that holds the whole Internet together is the network layer protocol, (71) . Unlike most older network layer protocols, it was designed from the beginning with internetworking in mind. Its job is to provide a (72) way to transport datagrams from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between them.

Communication in the Internet works as follows. The (73) layer takes data streams and breaks them up into datagrams. Each datagram is transmitted through the Internet, possibly being fragmented into smaller units as it goes. When all the pieces finally get to the destination machine, they are reassembled by the (74) layer into the original datagram. This datagram is then handed to the transport layer, which inserts it into the receiving process' input stream.

An IP datagram consists of a header part and a text part. The header has a (75) part and a variable length optional part.

(71)A. IP (Internet Protocol)

B. IP (Interworking Protocol)

C. TCP (Transport Control Protocol)

D. TCP (Transfer Communication Protocol)

(72)A. best-quality　　B. quality-guaranteed

C. connection-oriented　　D. best-efforts

(73)A. data link　　B. transport　　C. network　　D. application

(74)A. data link　　B. transport　　C. network　　D. application

(75)A. 40-byte fixed　　B. 64-byte fixed

C. 20~64-byte fixed　　D. 20-byte fixed

【答案】A　D　B　C　D

【解析】

将整个互联网连成一体的是网络层协议(71)。与大多数更早的网络层协议不同,它在设计之初就充分考虑了网络互连。它负责提供一种(72)的方式，从信源到信宿传递数据报，不管信源和信宿机器是否在同一个网络中，或者它们之间是否有其他网络。互联网中的通信遵

照以下方式进行。(73)层将数据流分割成数据报，每个数据报通过互联网传输的过程中，有可能被分割成更小的单元。当所有的数据单元最终到达目的地主机时，它们被(74)层重新组合成原始数据报。这个数据报随后被提交给传输层，由传输层将其插入接收进程的输入流中。一个 IP 数据报包含报头和报文两部分。报头包括一个(75)部分和一个可变长度的可选部分。

试题一

某企业最初只有一个办公地点，所有人员都集中在一个相对较小的封闭空间进行工作。由于是小型企业，社会影响不大，所以对安全性要求不高，主要目标是以最小的代价(费用)实现联网和访问互联网(Internet)，企业内部无对外提供的任何互联网服务。后来，随着企业不断发展，其网络建设也不断升级更新。(注：以下问题均不考虑无线网络技术)

【问题 1】

假定初期员工不超过 50 人，所有员工工作在同一楼层的不同房间，对互联网的访问带宽需求小于 2Mbps，且主要为进入企业内部的流量。

针对该企业网络建设，请从下面几个方面简要说明网络设计内容及依据：(1)网络结构；(2)物理层技术选择；(3)局域网技术选择；(4)广域网技术选择；(5)网络地址规划。

(1)因为网络规模较小，所以采用单核心局域网结构。配置一个核心二层或三层交换机，每个房间配备接入交换机。这种结构便于扩展和升级。

(2)物理层技术选择：通信介质选择 5 类 UTP 双绞线；网卡选择 10/100M 网卡。

(3)局域网技术选择：10/100/1000M 以太网技术。技术成熟，性价比最高，应用最广泛。

(4)广域网技术选择：由于初期无需对外提供互联网服务，入流量大于出流量，最佳接入技术是申请电信运营商的 ADSL 接入 Internet。

(5)地址规划：目前无需公网地址。采用私网地址即可。考虑初期人数最多 50 人，使用一个 C 类地址即可。如果每个房间需要隔离，可以使用 VLAN 并划分 IP 子网。

网络规划与设计过程一般会经历需求分析、逻辑网络设计、物理网络设计、规划及实施阶段。本题重点考查需求分析、逻辑网络设计这两个方面。

逻辑网络设计工作包括：网络结构设计：物理层技术选择；局域网技术选择；广域网技术选择；地址设计与命名模型；路由选择协议；网络管理：网络安全和逻辑网络设计文档。在逻辑网络设计方面，本题侧重考查网络结构设计、局域网技术选择、广域网技术选择、网络地址规划以及可扩展性网络结构设计方面的问题。

1.逻辑网络设计原则 .

根据用户需求设计逻辑网络，选择正确的网络技术比较关键，在选择时应考虑如下因素：

•通信带宽

所选择的网络技术必须保证足够的带宽，能够为用户访问应用系统提供保障；在进行选择时，不能仅局限于现有的应用要求，还要考虑适当的带宽增长需求。

•技术成熟度

所选择的网络技术必须是成熟稳定的技术，有些新的应用技术在尚没有大规模投入应用时，还存在着较多的不确定因素，而这些不确定因素可能会为网络的建设带来很多不可估量的损失。虽然新技术的自身发展离不开工程应用，但是对于大型网络工程来说，项目本身不能成为新技术的实验田；因此，使用较为成熟、拥有较多案例的技术是明智的选择。

当然，在面对技术变革时，可采用试点的方式逐步应用。

•连接服务类型

连接服务类型是逻辑设计时必须考虑的问题，传统的连接服务分为面向连接服务与非连接服务，逻辑设计需要在无连接和面向连接的协议之间进行权衡。

互联网采用 TCP/IP 协议簇，其网络层协议是 IP 协议，提供无连接的服务，因此选择连接服务类型，主要是针对 IP 协议底层的承载协议进行选择。如果选择面向连接服务类型，则可以选择 ATM、SDH 等协议；如果选择非连接服务类型，则可以选择以太网等协议。不同的网络工程，对连接服务类型的需求不同，设计者不能仅局限于一种连接服务而进行设计。

•可扩展性

网络设计者的设计依据是较为详细的需求分析，但是在选择网络技术时，不能仅考虑当前的需求，而忽视未来的发展；在大多数情况下，设计人员都会在设计中预留一定的冗余，无论是在带宽、通信容量、数据吞吐量、用户并发数等方面，网络实际需求和设计目标之间的比例应小于一个特定值以便于未来的发展;一般来说，这个值介于 70%～80%之间，在不同的工程中，可根据需要进行调整。

•高投资产出

选择网络技术的最关键一条，不是技术的扩展性、高性能，也不是成本最低等概念，决定设计和网络管理人员采用某种技术的最关键点是技术的投入产出比，只有通过投入产出分析，才能最后决定技术的使用。

2.网络结构设计

网络结构是对网络进行逻辑抽象，描述网络中的主要连接设备和计算机结点分布而形成的网络主体框架。网络结构和网络拓扑结构的最大区别在于：网络拓扑结构中，只有点和线，不会出现任何的设备和计算机结点；网络结构主要是描述连接设备和计算机结点的连接关系。由于当前的网络主要由局域网和实现局域网互联的广域网构成，因此可以将网络工程中的网

络结构设计分为局域网结构和广域网结构两个设计部分，其中局域网结构主要关注数据链路层的设备互连方式；广域网结构主要关注网络层设备的互连方式。

3.局域网结构

•单核心局域网结构

由一台核心三层交换机设备为中心构建的一种局域网结构，计算机结点通过多台接入交换机接入核心。整个局域网通过核心交换机与公共的互联网相连。

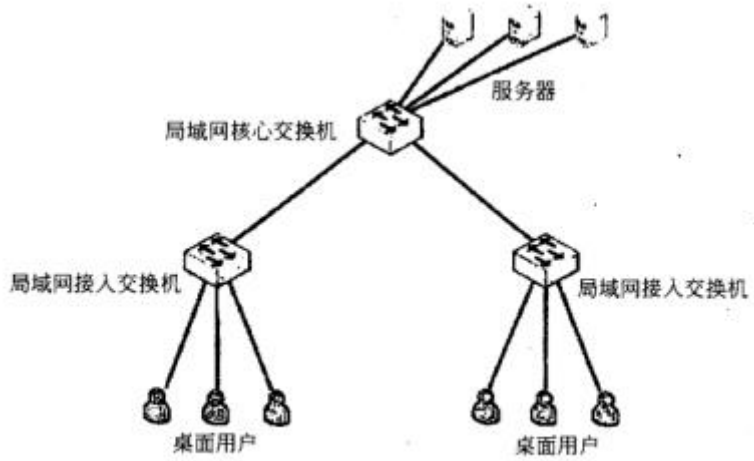


图 1-1 单核心局域网结构

•单核心结构局域网的主要特点：

(1)一台核心交换设备，路由功能只存在于核心设备上；

(2)结构简单，管理维护方便；

(3)投资小；

(3)网络覆盖范围小，要求网络分布比较紧凑；

(4)核心设备故障将导致网络瘫痪；

(5)可扩展为双核心局域网结构或层级结构的局域网。

•双核心局域网结构

双核心结构主要由两台三层交换机设备构建局域网核心。核心交换机与公共互联网相连。局域网内部的计算机结点通过接入交换机接入核心。

•双核心结构局域网的主要特点：

(1)两台核心交换设备组成局域网核心，路由功能只存在于局域网核心；

(2)核心设备之间运行特定的网关保护或负载均衡协议，如 HSRP、VRRP、GLBP 等；

(3)网络结构可靠性高；

(3)设备投资比单核心高；

(4)网络覆盖范围较大，取决于核心设备之间互联的技术；

(5)可升级为层次局域网结构。

双核心典型结构如图 1-2 所示。

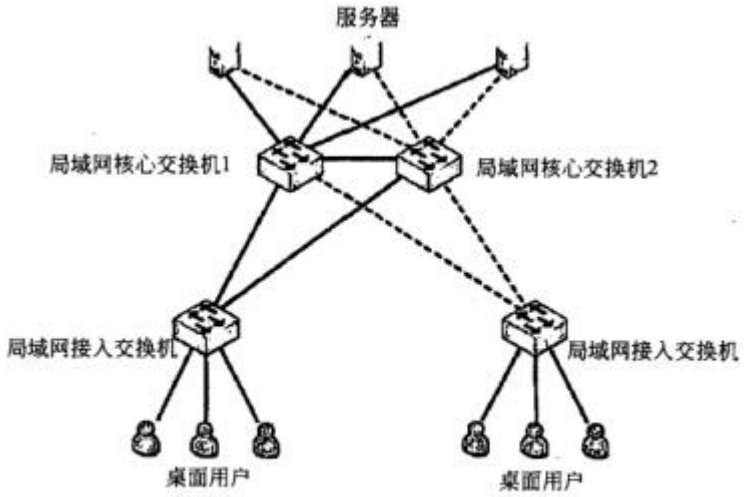


图 1-2 双核心局域网结构

•环型局域网结构

环型局域网结构有多台核心三层设备连接成双 RPR 动态弹性分组环，构建整个局域网的核心。环型结构的局域网应用较少，其典型结构如下：

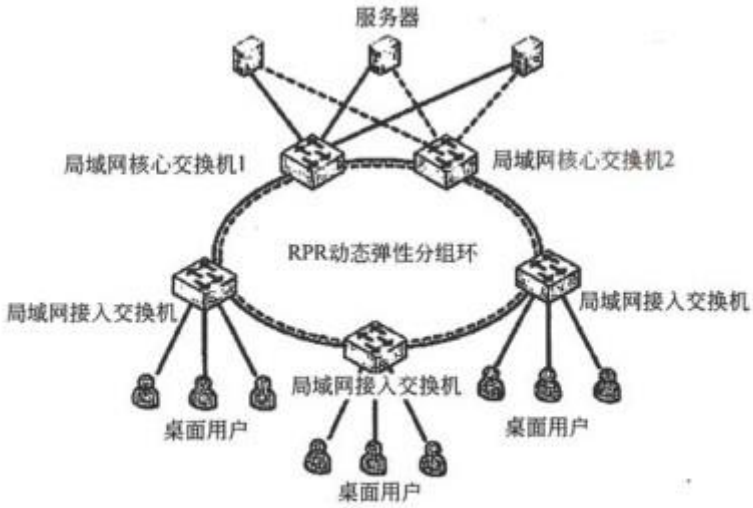


图 1-3 环型局域网结构

•层次局域网结构

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定义为核心层、汇聚层、接入层。其典型结构如图 1-4 所示。

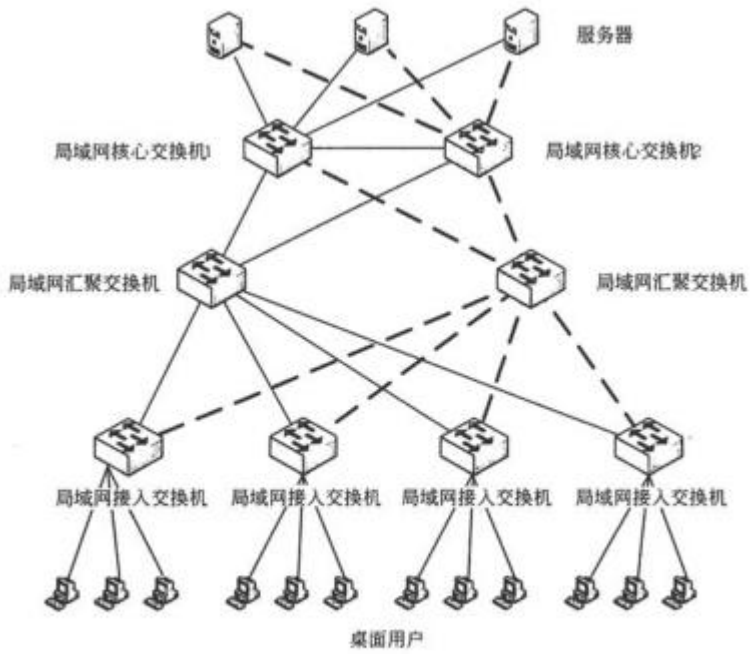


图 1-4 层次局域网结构

•层次局域网主要特点

(1)核心层实现高速数据转发；

(2)汇聚层实现丰富的接口和接入层之间进行互访控制；

(3)接入层实现用于接入；

(4)网络拓扑结构故障定位可分级便于维护；

(5)网络拓扑利用扩展；

(6)适用于大型的网络结构；

(7)网络投资大。

4.广域网结构

典型的广域网结构有：单核心广域网结构、双核心广域网结构、环型广域网结构、半冗余广域网结构以及层次子域广域网结构。

广域网组网主要应用于大型的电信服务公司组网以及大型的跨国公司组网。

5.局域网技术选择

目前可以使用的局域网技术有 IEEE802 系列局域网技术、FDDI 技术和 ATM 技术，其中 IEEE802 系列局域网技术主要有 IEEE802.3。

从逻辑网络设计原则看，最佳的选择技术是 IEEE802.3，即以太网技术。以太网技术的主要优势是：技术成熟；性价比高；组网、管理方便；支持多种速率和通信介质；支持除环型局域网以外的其他局域网结构。

6.广域网技术选择

就企业网来说，主要考虑企业网如何接入 Internet，因此就本题的广域网技术选择来说，就是选择公共 Internet 的接入技术。

从需求看，企业初期网络规模小，地理位置集中。可选择单核心结构的局域网结构。随着企业规模的扩大，可以升级为双核心结构或层次结构。从逻辑网设计原则看，局域网技术选择以太网技术。

以太网技术有：

•10Mpbs 以太网技术

具体连网可选择 10Base-T 全双工、半双工交换式连接以及共享式连接；

•100Mbp 以太网技术

100Base-TX 全双工、半双工交换式以及共享式连接。

100Base-FX 全双工、半双工交换式以及共享式连接。

•1000Mbps 以太网技术

1000Mbps 以太网简称 GE，它是目前建设高速 LAN 的主要技术之一，其标准为 802.3zo 千兆以太网标准出现之前，局域网主干采用 FDDI 或 ATM 技术。FDDI 是基于光纤的 100Mbps 局域网技术，是一个很成熟的技术，但价格相对较高。ATM 可以提供从 155Mbps 以上的带宽，但技术复杂，设备价格高，维护管理复杂。100M 以太网技术用于组建骨干局域网，其性能和速率均显不足。千兆以太网的几种规范及应用领域如下表所示：

标准名称	节质类型	线缆直径	最大传输距离	主要应用领域
1000Base-SX	多模光纤	62.5 μm	260 m	适合大楼主干网
1000Base-SX	多模光纤	50 μm	525 m	适合大楼主干网
1000Base-LX	多模光纤	62.5 μm	550 m	适合大楼主干网
1000Base-LX	多模光纤	50 μm	550 m	适合大楼主干网
1000Base-LX	单模光纤	9 μm	3000 m	校园或城域网骨干
1000Base-T	5类UTP		100 m	适合大楼主干网
1000Base-CX	150Ω STP		25 m	集群网络设备互联

以太网连网主要设备有：交换机。

广域网接入技术分析如下：

单独考查 Internet，可以把接入 Internet 的技术分为两类：一类是传统的接入技术，一类是新兴的接入技术。

传统的接入技术有：

•使用 Modem 经 PSTN 网络接入因特网。

•专线接入。租用电信公司(NSP)的线路接入因特网。

•局域网接入。由本地局域网直接接入因特网。

•无线接入。通过无线网络接入因特网。

新兴的接入技术主要有：

•ADSL 技术。采用数字用户线技术通过电话线实现因特网接入。

•HDSL 技术。另一种采用数字用户线技术，通过电话线实现因特网接入。

•HFC 技术。通过 CATV 网络接入因特网。

•光纤接入技术。以光纤为介质在用户和局端传输信息。

目前，针对企业用户，可以选择的接入技术主要是：ADSL 技术、专线技术、局域网接入和光纤接入。

ASDL 技术；上行速率最大 640Kbps，下行速率最大 8Mbps。主要特点：使用方便、投资少，适合主要为 Web 访问的网络；内部网络中不适合设置能对外提供公共服务的服务器。

专线接入：上下行速率相同。需要向电信部门(NSP)申请通信链路，通信链路一般是由 FR 帧中继网络和 DDN 网络提供的。专线入网一般通过路由器把用户端和局端相连。专线入网有以下特点是：采用租用专线作为数据传输的通道；租用专线以包 i 制计费，费用较高：专线入网提供 64Kbps～100Mbps 的传输速率；适合小的集团用户。

局域网接入：本地局域网直接通过路由器与 Internet 相连。局域网接入的特点是：可以利用局域网本身的各种优点；可接入大量用户：通信速率高；可靠性高；费用适中；(平均分配到每个用户)；局域网本身自成体系，方便管理：适合大量的集群用户，如用户小区等。局域网接入需要一定的条件才能实现，即局域网和公共广域网设备在同一个地理位置。比如在一个校园内，校园本身是一个大型的局域网，而本校园又是 Internet 的一个区域结点，公共广域网设备就在校园内。

光纤接入：本地局域网通过光纤接入公共的 Internet。特点：通信速率高；扩展性好；可靠性高：费用最贵；适合对通信带宽、质量要求较高的用户选择。

总结：采用单核心交换式以太网；选择 10/100MbpS 自适应物理层；选择 ADSL 作为接入技术；50 人采用一个 C 类网(私有地址)即可，无需划分子网。

【问题 2】

假定企业发展为中等规模，人数不超过 1000 人，所有员工在同一城市的不同地域工作。企业目前分为一个总部和三个分部(分布范围都不超过 2km)，总部人数不超过 400 人，分部人数不超过 200 人。企业与互联网采用统一对外接口，带宽需求规模为 100Mbps 以内，且流入数据量和流出数据量基本均衡；企业总部和分部之间的数据流量小于 1000Mbps。由于企业规模较大，对网络的依赖度大大增加，要求分部到总部和总部至互联网出口有备份，以增加网络的健壮性和可用性。

请从下面 3 个方面简要给出总部/分部网络和企业整体网络的结构和设计要点：(1)网络结构；(2)物理层和局域网技术选择；(3)接入互联网技术选择。

(1)网络结构设计：

总部局域网和分部局域网可以采用双核心局域网结构。

企业整体网络采用分层局域网结构，配备双核心路由器对外与互联网相连，对内与分部局域网的双核心交换机或路由器相连。

(2)物理层和局域网技术选择

总部局域网和分部局域网采用：10/100/1000M 以太网技术。通信介质可使用 5 类 UTP 双绞线或多模光纤。

总部局域网和分部局域网之间互联采用：1000BaseZX 以太网技术。通信介质：单模光纤。

(3)接入互联网技术选择

最佳方式：100Mbps 以太网接入。

其他可选方式：1000Mbps 以太网接入以及光纤接入(EPON)。

本问题主要考查网络扩展问题。现在企业分为 4 个部分，对应 4 个局域网：从整体网络结构上看，可以选择的是：双核心局域网结构和层次局域网结构。针对企业整体网络结构，1000 人的企业应该属于中、大型企业，企业整体网络结构优先选择层次局域网结构(骨干层：双核心路由器，提供与公共 Internet 的双链路连接；汇聚层：分部的双核心路由器；接入层：分部的接入交换机)；企业分部(或总部)内的局域网，从可靠性要求上看，应选择双核心局域网结构(对应层次结构的汇聚层和接入层，汇聚层选择双核心)。

可靠性除考虑可靠的网络结构外，企业骨干层设备之间、局域网骨干设备之间以及骨干设备和局域网骨干设备之间应考虑采用 GE 光纤连接(单模光纤最远 3km，如使用新的光收发器，最远可达 70km，满足地理覆盖分布要求)。

分部和总部内的局域网接入交换机仍采用 10/100Mbps 自适应 5 类 UTP 连接。

Internet 接入技术可选择双 100Mbps 光纤局域网接入或 1000Mbp 光纤局域网接入。其他 100Mbps 以上、可靠的接入技术也可选择。(100Mbps 以太网接入，从综合效益上看是最佳选择)。

【问题 3】

如果企业规模扩大到10000人，需要对外提供互联网服务(服务器的域名与IP一一对应)，对内提供企业内部服务，并允许员工访问互联网。假定企业总部和分部数量有 50 个，总部最多 500 人，分部最多 400 人。企业组织机构有 10 个(如行政管理、生产、销售等)，每个机构在总部或单个分部最多 60 人。

(1)请简要分析该企业网络的网络地址类型及规模。

(2)考虑管理便利、信息相互隔离和路由聚合等因素，请说明应如何规划 i1 企业网络的子网层次。

(3)举例说明如何进行子网划分(子网划分举例必须能够看出子网划分的规律，至少给出三个以上的子网号)。

(1)由于公司员工总数为 10000 人，考虑每人平均一个 IP 地址再加上公用设备地址、服务器地址等公用地址，可使用一个 B 类网。可以选择 172.16.0.0/16～172.32.0.0/16 中的任意一个。

(2)首先需要对 B 类网划分 50 个以上的子网。这 50 个子网要满足两个条件：每个子网能包含 500 以上的可用 IP 地址，并且能继续划分为 10 个子网，再次划分的 10 个子网，每个子网要能.包含 60 个可用的 IP 地址。

(3)举例

以 172.16.0.0/16 为例

采用/22 或 255.255.252.0 的子网掩码，可以把 B 类网划分为 64 个子网。(满足总部加分部 50 个)

172.16.0.0/22

172.16.4.0/22

…

172.16.252.0/22

每个子网再可划分 16 个子网：(满足每个总部或分部有 10 个部门)

以 172.16.4.0/22 为例：

172.16.4.0/26

172.16.4.64/26

每个子网可以包含最多：62 个 IP 地址(满足每个人一个 IP 地址)。

问题 3 重点考查地址规划和信息隔离问题。

局域网上的信息隔离可以使用 VLAN 技术来解决；

子网划分总体需求是：

•总体规模：

10000 人，至少每人一个 IP 地址；

其他地址：公共服务器地址；网络互联设备地址等。

考虑使用一个 B 类网。最多可容纳 65534 个 IP 地址。

•总部+分部子网数：

50 个，每个包含 500 以上地址(可考虑 20%余量)

考虑：B 类网中增加 6bit 子网 ID:包含 64 个子网。每个子网最多可包含 1022 个 IP 地址。

•总部或分部内部子网数：

10 个；最多 60 个地址

考虑：再增加 4bit 子网 ID，每个子网可再分为 16 个子网。每个子网最多可包含 62 个 IP 地址。

试题二

某单位的计算机网络结构如图 2-1 所示。

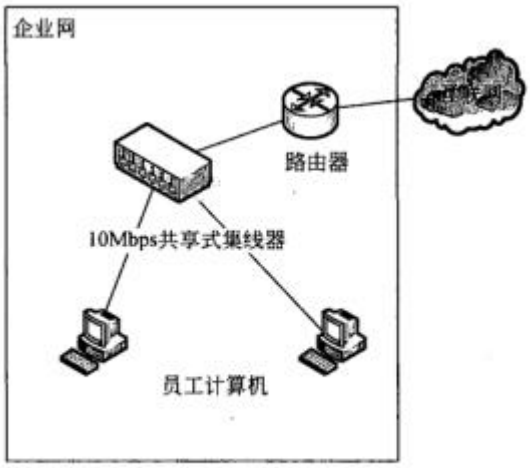


图 2-1 一个简单的初级网络

【问题 1】

如果单位想把员工分组，每组的信息相互隔离，另外保证每个员工能独享 10Mbps 带宽，请指出：

最简单的升级方式是什么？对新设备的功能和性能有什么要求(接入的计算机数量不大于 20 个，要说明如何实现分组的信息隔离)。

(1)用二层交换机取代 10M 共享式集线器。

(2)二层交换机需要支持 VLAN 功能，通过 VLAN 的划分，不同的 VLAN 对应不同的员工组，VLAN 之间的信息相互隔离。

(3)VLAN 策略可以通过基于交换机物理端口的策略来划分。接入不同端口的员工加入不同的 VLAN，即加入了不同的组。

(4)对交换机性能方面，可以使用 24 端口的 10/100Mbps 自适应以太网交换机。

(5)背板交换容量最低应达到 10×24/2=120Mbps。如果考虑所有端口 100Mbps 速率，则背板交换容量最低应达到 1.2Gbps。

试题二重点考查网络规划设计中的通信流量分析和依据流量对网络设备的选择。

本问题主要考查对 VLAN、共享式以太网、交换式以太网的理解。

VLAN 可以把 LAN 划分成逻辑上信息隔离的区域；

共享式以太网连接时，连接在共享式集线器(HUB)上的所有计算机站点共享相同的带宽。交互式以太网连接需要二层以太网交换机，每个端口连接一个计算机设备。交换式以太网可以实现独享带宽。VLAN 的划分必须是基于二层交换设备。集线器(HUB)不支持 VLAN 功能。VLAN 的实现策略有很多种类，最简单的是基于二层交换机的物理端口划分 VLAN。其他 VLAN 划分策略还有：基于 MAC 地址；基于 IP 地址或协议等。

交换机性能计算原则：一个端口连接一台计算机。背板交换容量计算公式是：交换机的背板交换容量=(交换机的端口数/2)×每端口的标称速率×全双工系数。如果交换机支持全双工，则全双工系数为 2;如果只支持半双工，全双工系数为 1。

二层交换机的端口数量一般是 8、16、24、48。20 台计算机可选择 24 端口的交换机。

【问题 2】

随着单位规模的扩大，企业网络发展成了如图 2-2 所示的结构。公用服务器均位于主网段。主网段没有用户，均为公用设备。用户均匀分布在网段 1、网段 2 和网段 3。

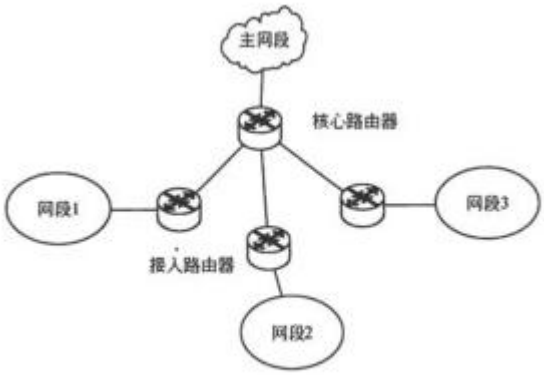


图 2-2 公司规模扩大后的网络结构

假定条件如下：

•网段 1、2、3 大致相同，不考虑协议封装的开销。

•用户收发邮件量大体相同。

•内部交流属于用户之间的 P2P 流量，80%的流量发生在网段内部用户之间，20%的流量发生在不同网段的用户之间，且平均分配流量。

•办公系统均为用户访问服务器，按上、下行不对称的一般原则分配流量。

•视频监控流量按用户比例在不同网段之间平均分配，属于 P2P 流量。

请根据表 2-1 中已有的信息将出流量、入流量和网内流量填写完整；将表 2-2 的目的网段和总流量填写完整。

表 2-1 网段 2 用户流量分析表

业务种类	平均用户数	每用户平均流量	总流量	出流量	入流量	网内流量
邮件	150	0.32Mbps	48Mbps			
办公系统	300	0.16Mbps	48Mbps			
视频监控	20	2.4Mbps	48Mbps			
内部交流	600	0.008Mbps	4.8Mbps			

表 2-2 网段 2 的总流量分配表

流量分布	源网段	目的网段	总流量
网段内部	2		
访问服务器	2		
服务器反馈	主网段		
P2P	2		

网段 2 用户流量分析表。

业务种类	出流量	入流量	网内流量
邮件	24Mbps	24Mbps	无
办公系统	9.6Mbps	38.4Mbps	无
视频监控	16Mbps	16Mbps	16Mbps
内部交流	0.48Mbps	0.48Mbps	3.84Mbps

网段 2 的总流量分配表。

流量分布	目的网段	总流量
网段内部	2	19.84Mbps
访问服务器	主网段	33.6Mbps
服务器反馈	2	62.4Mbps
P2P	网段 1 或网段 3	32.96Mbps

1.通信流量分布的简单规则

在通信规范分析中，最终的目标是产生通信量，其中必要的工作是分析网络中信息流量的分布问题。在整个过程中，需要依据需求分析的结果来产生单个信息流量的大小，依据通信模式、通信边界的分析，明确不同信息流在网络不同区域、边界的分布，从而获得区域、边界上的总信息流量^

对较为简单的网络，可以不需要进行复杂的通信流量分布分析，仅采用一些简单的方法，

例如 80/20 规则、20/80 规则等；但是对于复杂的网络，仍必须进行复杂的通信流量分布分析。

2.80/20 规则

80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：在一个网段中，通信流量的 80%是在该网段内流动，只有 20%的通信流量是访问其他网段。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

3.20/80 规则

随着互联网的发展，一些特殊的网络不断产生，例如小区内计算机用户形成的局域网、大型公司用于实现远程协同工作的工作组网络等。这些网络的特征就是：网段的内部用户之间相互访问较少，大多数网络访问都是对网段外的资源进行访问。对应这些流量分布则位于另一个极端，可以采用 20/80 规则。

20/80 规则的思路是：根据对用户和应用需求的统计，计算网段内的通信总量，其中 20%的通信流量是在该网段内流动，80%的通信流量是访问外部网段。

80/20 规则和 20/80 规则虽然比较简单，但这些规则是建立在大量的工程经验基础上的；另外通过这些规则的应用，可以很快完成一个复杂网络中大多数网段的通信流量分析工作，可以合理减少大型网络中的设计工作量。

4.通信流量分析步骤

步骤一：把网络分成易管理的网段。

步骤二：确定个人用户和网段应用的通信流量。

步骤三：确定本地和远程网段上的通信流量^

步骤四：对每个网段重复步骤一、步骤二、步骤三。

步骤五：分析基于各网段信息的广域网和骨干网络的通信流量。

5.常见互联网业务流量规则。

E-mail：发送邮件和接收邮件(只与邮件服务器发生流量)。视为对等流量，即 50%流出，50%流入。

Web：浏览网络，从 Web 下载的流量大(只与 Web 服务器发生流量)。使用 20/80 法则。流出 20%，流入 80%。

FTP 或文件共享业务：等同电子邮件业务(只与 FTP 或文件共享服务器发生流量)。流入、流出各 50%。

办公自动化业务：等同 Web 业务(只与办公自动化服务器发生流量)。20%流出，80%流入。

视频监控：属于 P2P 业务类型(用户之间发生流量)，在内部网络中流量平均分配。内部交流：属于 P2P 业务类型(用户之间发生流量)，80%发生在网段内部，20%发生在网段之间。

根据问题 2 给出的条件。网段 2 的流量计算如下：

电子邮件业务：总流量 48Mbps，50%流出本网段 24Mbps，50%流入本网段 24Mbps。无内部流量。

办公系统：总流量 48Mbps，20%流出本网段 9.6Mbps，80%流入本网段 38.4Mbps。无内部流量。

视频监控：总流量 48Mbps，三个网段平均分配，则外部流量占 2/3，即 32Mbps，流入流出各占 50%，即：流入 16Mbps、流出 16Mbps:网内流量占 1/3，即 16Mbps。

内部交流：总流量 4.8Mbps，20%网段之间流量，出入平均分配则流出：0.48Mbps、流入 0.48Mbps:80%网段内部，即 3.84Mbps。

【问题 3】

(1)请计算出接入路由器内部交换流量、网段至主网段流量、网段之间流量和总流量。

(2)请计算出核心路由器的出、入流量和总流量。

(3)在 10/100/1000Mbps 的局域网技术中，应该选择哪一个作为网段内部互联技术(说明对路由器交换容量的最小要求)？

(4)在 10/100/1000Mbps 的局域网技术中，应该选择哪一个作为网段至主网段互联技术(说明对路由器交换容量的最小要求)？

(5)如果主网段和网段之间协议开销最大可增加 20%流量，是否需要升级网络？如果需要升级，最佳方案是什么？如果不需要升级，请说明原因。

(1)接入路由器：网段内部交换流量：19.84Mbps 网段至主网段流量：48Mbps+48Mbps=96Mbps 网段之间流量：32.96Mbps

总流量：48×3+4.8=148.8Mbps

(2)核心路由器：

网段与主网段之间总流量：96Mbps×3=288Mbps；

其中：主网段到网段流量(出流量)：(24+38.4)×3=187.2Mbps；

网段到主网段流量(入流量)：(24+9.6)×3=100.8Mbps。

网段之间的转发流量：32.96Mbps×3=98.88Mbps 总流量：286.88Mbps

(3)网段内部选择 100Mbps 以太网技术，接入路由器背板交换容量在 200Mbps 以上。

(4)网段和主网段之间选择 100Mbps 以太网技术交互式连接，核心路由器背板交换容量在 400Mbps 以上。

(5)需要升级网络。核心路由器和接入路由器之间采用全双工 100Mbps 交换式连接。核心路由器背板交换容量 600Mbps 以上。

问题 3 依据问题 2 的流量分布进行计算。

按三个子网段相同来计算，以网段 2 为例。

接入路由器：

内部流量：

视频监控内部流量 16Mbps+内部交流内部流量 3.84Mbps

网段至主网段流量(出流量+入流量)：48+48=96Mbps

网段之间的流量(出流量+入流量)：32+0.96=32.96Mbps

总流量：48*3+4.8=148.8Mbps

核心路由器：

网段之间转发流量(出流量+入流量)：32.96Mbps*3=98.88Mbps

网段到主网段流量(出流量+入流量)：96Mbps*3=288Mbps 总流量：286.88Mbps

路由器背板交换容量选择原则：大于总流量，并有 20%～30%的冗余。取整为 200Mbps 的整数倍。

【问题 4】

参见本题图 2-2。如果要提高普通网段访问主网段的可靠性和可用性，即在核心路由器出现故障时仍能访问主网段，请简要说明应该增加什么设备，新增设备与核心路由器之间可使用哪些协议以及这些协议之间主要有何区别。

(1)再增加一个核心路由器。

(2)两个核心路由器之间运行 VRRP、HSRP 协议或 GLBP 协议。

VRRP 协议是公开的虚拟路由器冗余协议。HSRP 是 Cisco 开发的热备份路由协议。

(3)VRRP 和 HSRP 基本功能类似，其缺点是存在路由器闲置问题。GLBP 协议与 VRRP 和

HSRP 功能类似，但能够实现负载均衡功能。

本问题主要考查单核心局域网结构和双核心局域网结构在可靠性方面的区别，以及双核心局域网结构中核心设备之间重要的可靠性协议(冗余备份协议、流量均衡协议)。

单核心局域网结构的主要缺点是，核心结点故障将导致整个网络瘫痪(不可用)，增加可靠性和可用性的最佳方法是增加一台新的核心路由器。两台核心路由器之间运行 VRRP 协议、HSRP 协议或 GLBP 协议。

VRRP(Virtual Router Redundancy Protocol，虚拟路由冗余协议)是一种容错协议。通常，一个网络内的所有主机都设置一条缺省路由，这样，当主机发出数据包的目的地址不在本网段时，报文将被通过缺省路由发往网关路由器，从而实现了主机与外部网络的通信。当某网络的默认网关(路由器)故障时，本网段内所有主机将不能与外部网络通信。VRRP 就是为解决这一严重问题而提出的，它为具有多播或广播能力的局域网设计。VRRP 将局域网的一组路由器(包括一个Master即主控路由器和若干个Backup即备份路由器)组织成一个虚拟路由器，称之为一个备份组。

在 VRRP 协议中，有两组重要的概念：VRRP 路由器和虚拟路由器，主控路由器和备份路由器。VRRP 路由器是指运行 VRRP 的路由器，是物理实体，虚拟路由器是指 VRRP 协议创建的，是逻辑概念。一组 VRRP 路由器协同工作，共同构成一台虚拟路由器。该虚拟路由器对外表现为一个具有唯一固定 IP 地址和 MAC 地址的逻辑路由器。处于同一个 VRRP 组中的路由器具有两种互斥的角色：主控路由器和备份路由器，一个 VRRP 组中有且只有一台处于主控角色的路由器，可以有一个或者多个处于备份角色的路由器。VRKP 协议使用选择策略从路由器组中选出一台作为主控路由器，负责 ARP 响应和转发 IP 数据包，组中的其他路由器作为备份的角色处于待命状态。当主控路由器发生故障时，其中一台备份路由器能在几秒钟的时延后升级为主路由器。由于切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对用户是透明的。

HSRP 是 Cisco 开发的热备份路由协议，与 VRRP 基本功能类似。GLBP 协议与 VRRP 和 HSRP 功能类似，但能够实现负载均衡功能。

试题三

某机构打算新建一个网络，其中有内部办公计算机若干台，内部数据库服务一台，内部文件传输(FTP)服务器一台，网页(Web)服务器一台，邮件服务器一台。要求能对外提供万维网(WWW)访问和邮件服务，内部办公计算机和内部数据库、文件传输(FTP)服务器对外不可见。

【问题 1】

请划分该机构网络的安全区域和安全级别，说明各机器属于哪个区域和级别。

整个网络分为三个不同级别的安全区域：

1.内部网络：安全级别最高，是可信的、重点保护的区域。包括所有内部办公计算机，内部数据库服务器和内部 FTP 服务器。

2.外部网络：安全级别最低，是不可信的、要防备的区域。包括外部因特网用户主机和设备。

3.DMZ 区域(非军事化区)：安全级别中等，因为需要对外开放某些特定的服务和应用，受一定的保护，是安全级别较低的区域。包括对外提供 WWW 访问的 Web 服务器和邮件服务器。

本题涉及网络安全区域的划分、防火墙和入侵检测等的内容。

要保障一个网络系统的安全，首先应该分析该网络系统的特点和安全需求，分析对外需要提供的服务，评估需要保护的数据的安全级别和面临的风险，划分不同的安全区域，然后再制定系统安全策略，决定实现时采用何种方式和手段。

本题所述机构的网络中有内部数据库服务和内部文件传输(FTP)服务器各一台，内部办公计算机若干台。服务器上存储的数据信息量大，且是内部数据，安全级别要求最高，内部办公计算机处理的数据也是内部数据，不对外公开，其安全级别也可定位最高。因此这些机器应该统一划分在同一个安全区域，以便采用统一的安全策略来实施重点保护。

本题所述机构的网络中有网页(Web)服务器和邮件服务器各一台。由于要求能对外提供万维网(WWW)访问服务和邮件服务，则这两台服务器对本机构网络外部的设备是可见的，外部设备会访问这两台服务器，可能会受到外网不安全因素的威胁，其安全级别会降低。因此不能同内部服务器等放在同一区域，以免在遭受攻击时影响内部网络。因此这两台服务器应该统一划分在同一个安全区域，以便采用统一的安全策略来统一实施保护，以保证能对外提供正常的服务。

本机构网络之外的因特网设备和主机，能访问该机构网络中有网页(Web)服务器和邮件服务器，这部分设备和主机是不可信的、要防备的区域，安全级别最低，可划分为同一个安全区域。

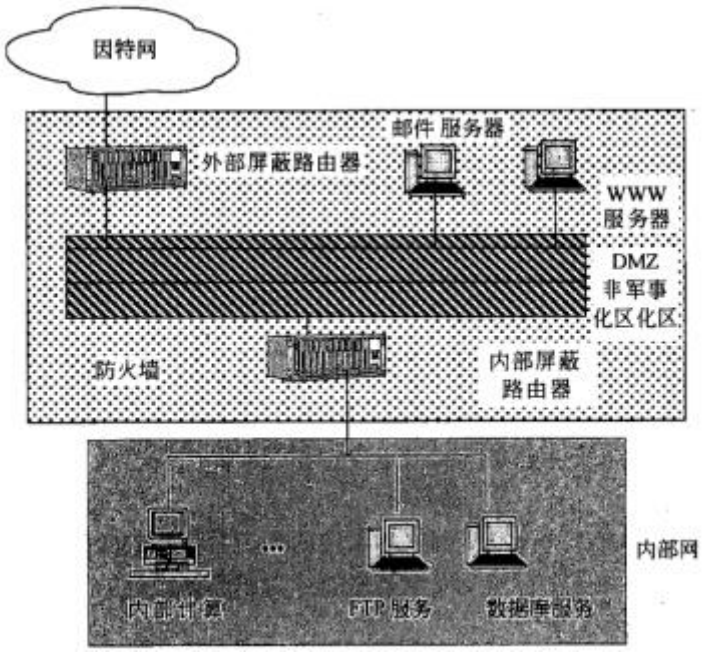
【问题 2】

为提高安全性，请设计该机构网络的防火墙方案，画出拓扑图，并给出防火墙的相关规则的配置策略。

配置策略：

外部屏蔽路由区的访问策略：允许外部网络客户访问 DMZ 区的 WWW 服务器提供的 WWW 服务和邮件服务器提供的邮件服务，其他禁止：

内部屏蔽路由器的访问策略：允许内部网客户访问外部网络，不允许外部网络客户访问内部网；允许内部网客户访问 DMZ 区，不允许 DMZ 区网络客户访问内部网。



防火墙的典型体系结构(部署方式)有三种形式：双重宿主主机体系结构、屏蔽主、机体系结构、屏蔽子网体系结构，具体部署时需根据网络的特点和具体的安全需求、安全策略来决定。

防火墙的双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络和内部网络的任务。一个典型的双宿主主机防火墙如图 3-1 所示，它使用一个

双宿主主机完成防火墙功能。该主机至少有两个网络接口，一个是内部网络接口，一个是因特网接口，故称为双宿主主机。

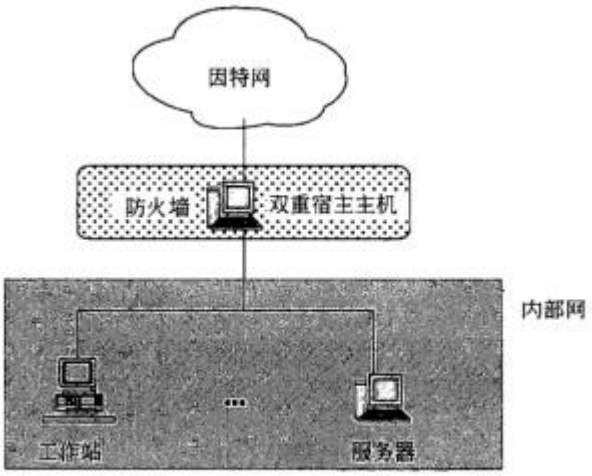


图 3-1 双宿主主机结构防火墙

防火墙的屏蔽主机体系结构如图 3-2 所示，通过屏蔽路由器和堡垒主机结合的方式来构造防火墙。其中屏蔽路由器是一个单独的路由器，采用包过滤方式来实现内、外部网络的隔离和对内网的保护，而堡垒主机是因特网中的主机能够访问的唯一的内部网中的主机，内部网中的其他主机对外都是不可见的，故称为屏蔽主机防火墙。

堡垒主机通常是安全管理员标识的作为网络安全中关键点的系统，这类系统健壮安全，能抗攻击，故称为堡垒主机。在屏蔽主机防火墙中，堡垒主机用于对外提供一定的服务，如 WWW 服务，而 1 任何外部的主机只有通过这台主机才能得到内部系统的服务(在外部主机看来，没有内部网络，只有堡垒主机)。由于堡垒主机暴露在因特网中，故堡垒主机需保持较高的安全等级，具有一定的抗攻击能力。

防火墙的屏蔽子网体系结构的最简单形式如图 3-3 所示，防火墙由外部屏蔽路由器、内部屏蔽路由器和堡垒主机共同组成。与前两种防火墙体系结构有明显区别的是，在外/内部屏蔽路由器间有一个称为非军事化区的子网，进一步将内部网络同因特网隔离开来，起到屏蔽内部网络的作用，提供更进一步的安全性，故称为屏蔽子网防火墙。

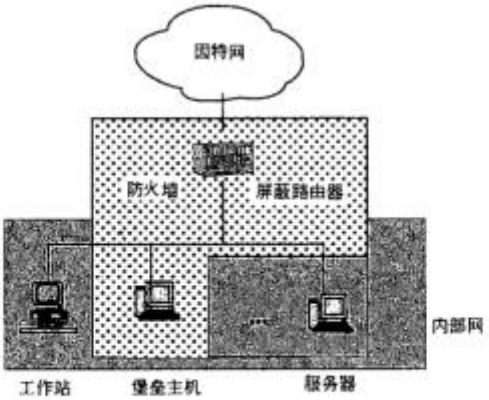


图 3-2 屏蔽主机体系结构防火墙

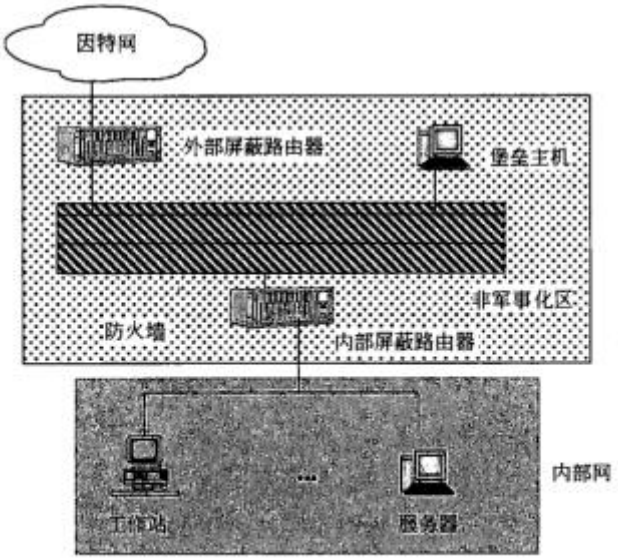


图 3-3 屏蔽子网结构防火墙

非军事化区即 DMZ: De-Militarized Zone，原指古代战场上交战双方的开火区及后方保护区之间的隔离地带，在该隔离地带中，会有一些冲突和一定的危险，但危害性不大且容易控制，而且在大规模战争爆发前能及时告警。此概念用于网络安全中是指额外的安全保护子网，信任度较低、易受攻击的对外提供服务的服务器和堡垒主机都放置在该子网中，远离内部网络。DMZ 概念的出现源于用户对防火墙使用中的需求，早期简单的防火墙提供的是内部网与外部网之间的边界保护，而内部网中对外提供服务的服务器(如邮件服务器)比其他的内部网的机器遭到入侵的可能性要高很多，且这些服务器一旦被入侵，将被用来做为跳板攻击整个内部网。有了非军事化区后，一旦入侵者侵入非军事化区，最坏会损坏其中的服务器和堡垒主机，但不会损伤到内部网的完整性，而且通过在周边网络上隔离对外提供服务的服务器和堡垒主机，还减少了网络安全对堡垒主机的依赖。非军事化区中的主机主要通过主机安全来保证其安全性。

屏蔽子网防火墙使用了两个屏蔽路由器，消除了内部网络的单一侵入点，增强了网络的

安全性。但两个屏蔽路由器的规则设置的侧重点不同。

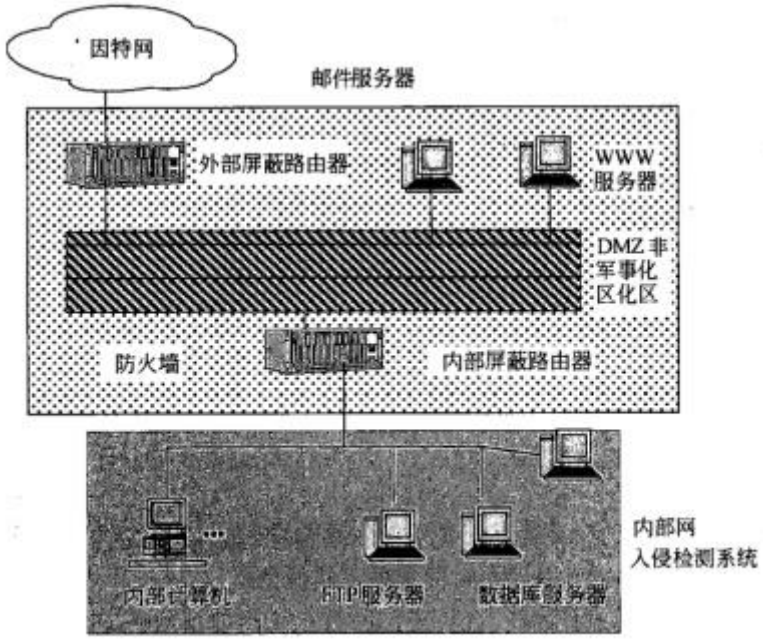
配置防火墙的访问策略时，一般按服务来配置规则。首先要分析网络的特点及网络对外提供的服务，弄清各服务的工作原理及正常的工作流程，然后再分析各服务在防火墙环境下如何工作，并对服务配置。

【问题 3】

如果想要监听、检测内部办公计算机之间的连接和攻击，应该在何位置配置何种设备？画出相关拓扑图。

(1)应该配置入侵检测系统(IDS 系统)。

(2)拓扑图为：



防火墙和操作系统加固技术等传统安全技术都是静态安全防御技术，不能提供足够的安全性：入侵检测系统能使系统对入侵事件和过程做出实时响应，提供系统的动态安全性。入侵检测系统是通过从计算机网络和系统的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定措施的技术。

入侵检测系统包括三部分内容：信息收集、信息分析和响应。其中收集信息的可靠性和

正确性在很大程度上决定了入侵检测系统的有效性和准确性。需要在合适的位置上放置，以保证采集信息的准确性和充足性。

试题一 论计算机网络系统设计中接入技术的选择

计算机网络技术的发展非常迅速，新技术不断涌现。在网络设计和实现中，各种接入方式和接入技术不断成熟，要求在网络规划和设计中，考虑实际情况，针对具体目标，选择适合的接入方式和技术。

请围绕“计算机网络系统设计中接入技术的选择”论题，依次对以下三个方面进行论述。

1.简要叙述你参与设计和实施的计算机网络项目，以及你所担任的主要工作和接入方式的选择。

2.详细论述你在网络规划和设计中接入技术选择的思路与策略，以及所采用的技术和方法。

分析和评估你所采用的接入技术的措施及其效果，以及相关的改进措施。

一、对 VPN 技术和方案的叙述要点

1. VPN 技术的概念

虚拟专用网（VirtualPrivateNetwork,VPN)就是建立在公用网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而通过 ISP 提供的公用网络来实现通信，其专用性表现在 VPN 之外的用户无法访问 VPN 内部的网络资源，VPN 内部用户之间可以实现安全通信。

2. 实现 VPN 的关键技术

隧道技术、加解密技术、密钥管理技术、身份认证技术。

3. VPN 的解决方案

(1) 内联网 VPN(IntranetVPN)：企业内部虚拟专用网也叫内联网 VPN，用于实现企业内部各个 LAN 之间的安全互联。

(2) 外联网 VPN(ExtranetVPN)：企业外部虚拟专用网也叫外联网 VPN，用于实现企业与客户、供应商和其他相关团体之间的互联互通。

(3) 远程接入 VPN(AccessVPN)：解决远程用户访问企业内部网络的传统方法是采用长途拨号方式接入企业的网络访问服务器（NAS)。这种访问方式的缺点是通信成本高，必须支付价格不菲的长途电话费，而且 NAS 和调制解调器的设备费用，以及租用接入线路的费用也是一笔很大的开销。采用远程接入 VPN 就可以省去这些费用。如果企业内部人员有移动或远程办公的需要，或者商家要提供 B2C 的安全访问服务，可以采用 AccessVPN。

4.虚拟专用网 VPN 的协议实现

隧道协议（例如 PPTP 和 L2TP），把数据封装在点对点协议（PPP)的帧中在互联网上传输，创建隧道的过程类似于在通信双方之间建立会话的过程，需要就地址分配、加密、认证和压缩参数等进行协商，隧道建立后才进行数据传输。

IPsec(IPSecurity)是 IETF 定义的一组协议，用于增强 IP 网络层安全。IPsecVPN 是在网络层建立安全隧道，适用于建立固定的虚拟专用网。

安全套接层（SecureSocketLayer,SSL)是传输层安全协议，用于实现 Web 安全通信。SSL 的安全连接是通过应用层的 Web 连接建立的，更适合移动用户远程访问公司的虚拟专用网。

二、叙述自己参与设计和实施的计算机网络项目，该项目应有一定的规模，自己在该项目中担任的主要工作应有一定的份量，说明项目中选用的 VPN 方案以及选用该方案的理由。

三、对选择的网络系统设计中 VPN 方案的效果以及需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

试题二 论计算机网络系统的可靠性设计

计算机网络规划和设计的可靠性问题是一个关键问题，是网络规划和设计所必须考虑的，其目的是提高网络系统的可靠性，保证网络系统的稳定运行。

请围绕“计算机网络系统的可靠性设计”论题，依次对以下三个方面进行论述。

1.简要叙述你参与的计算机网络项目和你所承担的主要工作，以及项目的可靠性要求。

2.从接入、网络、设备和系统等方面，讨论网络设计的可靠性的解决方案和措施。

3.评估在网络设计中你采用可靠性的措施所带来的好处和问题。

以你负责规划、设计及实施的校园网项目为例，概要叙述针对实际需求的设计要点，以及如何充分利用已有的软硬件，或对现有硬件资源的调优措施。

(1) 叙述自己参与设计和实施的计算机网络项目。该项目应有一定的规模，自己的主要工作应有-定的份量。

(2) 项目中对软硬件的重新利用及调优方案。已有软硬件资源不适合整个网络环境的应该淘汰，可以用在要求较低环境中的可重利用，更高要求的要重新购置。

二、具体讨论在校园网/企业网网络规划与设计中光纤连接关键技术、采用的无线技术及解决方案。

在光纤连接技术方面：

(1) 光纤连接的总体环境。在光纤网络部署时首先要考虑距离、所要求达致的速率。

(2) 介质选择。依据距离、速率以及成本选择采用单模还是多模，考虑室内或是室外选择不同的光纤。

(3) 接口模块与成本预算。在介质选择完成后，需要考虑光纤接口模块，计算成本。

(4) 冗余。考虑到光纤日后扩展及链路备份，需要冗余链路。

在无线技术方面：

(1) 无线网络需求。不同的无线网络环境需要不同的速率和安全要求，需要描述所涉及网络的要求环境。

(2) 采用的无线局域网络标准。不同的速率和安全要求需要采用不同的标准，注意选择标准与需求相匹配。

(3) 无线网络的网络结构及覆盖范围。

(4) 选用的无线接入设备，包括无线路由器、AP 等。

三、具体讨论在上述关键技术的实施过程中遇到的问题和解决措施，以及实际运行效果。

(1) 在光纤连接和无线技术使用过程中遇到的问题及解决措施。

(2) 网络部署完成后实际的效果、达到的性能。