计算机采用分级存储体系的主要目的是为了（1）。

(1)A.解决主存容量不足的问题

B.提高存储器读写可靠性

C.提高外设访问效率

D.解决存储的容量、价格和速度之间的矛盾

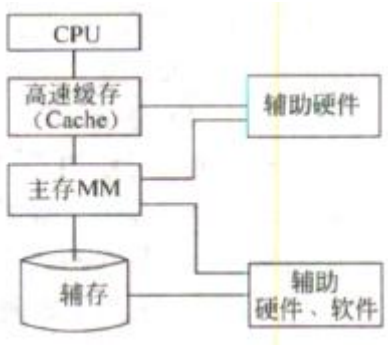
【答案】D

【解析】本题考查计算机系统基础知识。

存储体系结构包括不同层次上的存储器，通过适当的硬件、软件有机地组合在一起形成计算机的存储体系结构。

例如，由高速缓存（Cache)、主存储器（MM)和辅助存储器构成的3层存储器层次结构存如右图所示。

接近CPU的存储器容量更小、速度更快、成本更高；辅存容量大、速度慢，价格低。采用分级存储体系的目的是解决存储的容最、价格和速度之间的矛盾。



设关系模式R (U，F)，其中U为属性集，F是U上的一组函数依赖，那么函数依赖的公理系统(Armstrong公理系统)中的合并规则是指为（2）为F所蕴涵。

(2)A.若A→B，B→C，则A→C　　B.若Y⊆X⊆U，则X→Y

C.若A→B，A→C ,则A→BC　　D.若A→B，C⊆B,则A→C

【答案】C

【解析】本题考查函数依赖推理规则。

函数依赖的公理系统（即Armstrong公理系统）为：设关系模式R(U，F),其中U为属性集，F是U上的一组函数依赖，那么有如下推理规则：

A1自反律：若Y⊆X⊆U，则X→Y为F所蕴涵。

A2增广律：若X→Y为F所蕴涵，且Z⊆U，则XZ→YZ为F所蕴涵。

A3 传递律：若 X→Y，Y→Z 为 F 所蕴涵，则 X→Z 为 F 所蕴涵。

根据上述三条推理规则又可推出下述三条推理规则：

A4 合并规则：若 X→Y，X→Z,则 X→YZ 为 F 所蕴涵。

A5 伪传递率：若 X→Y，WY→Z,则 XW→Z 为 F 所蕴涵。

A6 分解规则：若 X→Y，Z⊆Y，则 X→Z 为 F 所蕴涵。

选项 A 符合规则为 A3,即传递规则；选项 B 符合规则为 A1，即为自反规则：选项 C 符合规则为 A4,即为合并规则；选项 D 符合规则为 A6,即为分解规则。

在结构化分析方法中，用（3）表示功能模型，用（4）表示行为模型。

(3)A.ER 图　　B.用例图　　C.DFD　　D.对象图

(4)A.通信图　　B.顺序图　　C.活动图　　D.状态转换图

【答案】C　D

【解析】

结构化分析方法的基本思想是自顶向下,逐层分解,把一个大问题分解成若干个小问题，每个小问题再分解成若干个更小的问题。经过逐层分解，每个圾低层的问题都是足够简单、容易解决的。结构化方法分析模型的核心是数据字典，围绕这个核心，有三个层次的模型，分别是数据模型、功能模型和行为模型（也称为状态模型)。在实际工作中，一般使用 E-R 图表示数据模型，用 DFD 表示功能模型，用状态转换图表示行为模型。这三个模型有着密切的关系，它们的建立不具有严格的时序性，而是一个迭代的过程。

以下关于单元测试的说法中，正确的是（5）。

(5)A.驱动模块用来调用被测模块，自顶向下的单元测试不需要另外编写驱动模块

B.桩模块用来模拟被测模块所调用的子模块，自顶向下的单元测试中不需要另外编写桩模块

C.驱动模块用来模拟被测模块所调用的子模块，自底向上的单元测试中不需要另外编写驱动模块

D.桩模块用来调用被测模块，自底向上的单元测试中不需要另外编写桩模块

【答案】A

【解析】本题考查单元测试的基本概念。

单元测试也称为模块测试，测试的对象是可独立编译或汇编的程序模块、软件构件或面

向对象软件中的类（统称为模块），其目的是检查每个模块能否正确地实现设计说明中的功能、性能、接口和其他设计约束等条件，发现模块内可能存在的各种差错。单元测试的技术依据是软件详细设计说明书。

测试一个模块时，可能需要为该模块编写一个驱动模块和若干个桩模块。驱动模块用来调用被测模块，它接收测试者提供的测试数据，并把这些数据传送给被测模块，然后从被测模块接收测试结果，并以某种可见的方式将测试结果返回给测试人员：桩模块用来模拟被测模块所调用的子模块，它接受被测模块的调用，检验调用参数，并以尽可能简单的操作模拟被调用的子程序模块功能，把结果送回被测模块。顶层模块测试时不需要驱动模块，底层模块测试时不要桩模块。

单元测试策略主要包括自顶向下的单元测试、自底向上的单元测试、孤立测试和综合测试策略。

①自顶向下的单元测试。先测试上层模块，再测试下层模块。测试下层模块时由于它的上层模块已测试过，所以不必另外编写驱动模块。

②自底向上的单元测试。自底向上的单元测试先测试下层模块，再测试上层模块。测试上层模块由于它的下层模块已经测试过，所以不必另外编写桩模块。

③孤立测试不需要考虑每个模块与其他模块之间的关系，逐一完成所有模块的测试。由于各模块之间不存在依赖性，单元测试可以并行进行，但因为需要为每个模块单独设计驱动模块和粧模块，增加了额外的测试成本。

④综合测试。上述三种单元测试策略各有利弊，实际测试时可以根据软件特点和进度安排情况，将几种测试方法混合使用。

公司欲开发一个用于分布式登陆的服务器端程序，使用面向连接的 TCP 协议并发地处理多客户端登陆请求。用户要求该服务端程序运行在 Linux、Solaris 和 Windows NT 等多种操作系统平台之上，而不同的操作系统的相关 API 函数和数据都有所不同。针对这种情况，公司的架构师决定采用“包装器外观（Wrapper Facade）”架构模式解决操作系统的差异问题。具体来说，服务端程序应该在包装器外观的实例上调用需要的方法，然后将请求和请求的参数发送给（6），调用成功后将结果返回。使用该模式（7）。

(6)A.客户端程序　　B.操作系统 API 函数

C.TCP 协议 API 函数　　D.登录连接程序

(7)A.提高了底层代码访问的一致性，但降低了服务端程序的调用性能

B.降低了服务端程序功能调用的灵活性，但提高了服务端程序的调用性能

C.降低了服务端程序的可移植性，但提高了服务端程序的可维护性

D.提高了系统的可复用性，但降低了系统的可配置性

【答案】B　A

【解析】本题主要考查考生对设计模式的理解与应用。

题干描述了某公司欲开发一个用于分布式登录的服务端程序，使用面向连接的 TCP 协议并发地处理多客户端登录请求。用户要求该服务端程序运行在 Linux、Solaris 和 Windows NT 等多种操作系统平台之上，而不同的操作系统的相关 API 函数和数据都有所不同。针对这种情况，公司的架构师决定采用“包装器外观（WrapperFacade)”架构模式解决操作系统的差异问题。具体来说，服务端程序应该在包装器外观的实例上调用需要的方法，然后将请求和请求的参数发送给操作系统 API 函数，调用成功后将结果返回。使用该模式提高了底层代码访问的一致性，但降低了服务端程序的调用性能。

某服装店有甲、乙、丙、丁四个缝制小组。甲组每天能缝制 5 件上衣或 6 条裤子：乙组每天能缝制 6 件上衣或 7 条裤子：丙组每天能缝制 7 件上衣或 8 条裤子；丁组每天能缝制 8 件上衣或 9 条裤子。每组每天要么缝制上衣，要么缝制裤子，不能弄混。订单要求上衣和裤子必须配套（每套衣服包括一件上衣和一条裤子）。做好合理安排，该服装店 15 天最多能缝制（8）套衣服。

(8)A.208　　B.209　　C.210　　D.211

【答案】D

【解析】本题考查数学应用能力

根据题意，甲、乙、丙、丁四组做上衣和裤子的效率之比分别为 5/6、6/7、7/8、8/9，并且依次增加。因此，丁组做上衣效率更高，甲组做裤子效率更高。为此，安排甲组 15 天全做裤子，丁组 15 天全做上衣。

设乙组用 x 天做上衣，15-x 天做裤子；丙组用 y 天做上衣，15-y 天做裤子，为使上衣和裤子配套，则有

0+6x+7y+8*15=6*15+7(15-x)+8(15-y)+0

所以，13x+15y=13*15，y=13-13x/15

15 天共做套数 6x+7y+8*15=6x+7(13-13x/15)+120=211-x/15

只有在 x=0 时，最多可做 211 套。

此时，y=13，即甲乙丙丁四组分别用 0、0、13、15 天做上衣，用 15、15、2、0 天做裤子。

生产某种产品有两个建厂方案。(1）建大厂：需要初期投资 500 万元。如果产品销路好，每年可以获利 200 万元；如果销路不好，每年会亏损 20 万元。(2）建小厂，需要初期投资 200 万元。如果产品销路好，每年可以获利 100 万元；如果销路不好，每年只能获利 20 万元。市场调研表明，未来 2 年，这种产品销路好的概率为 70%。如果这 2 年销路好，则后续 5 年销路好的概率上升为 80%;如果这 2 年销路不好，则后续 5 年销路好的概率仅为 10%。为取得 7 年最大总收益，决策者应（9)。

(9)A.建大厂，总收益超 500 万元　　B.建大厂,总收益略多于 300 万元

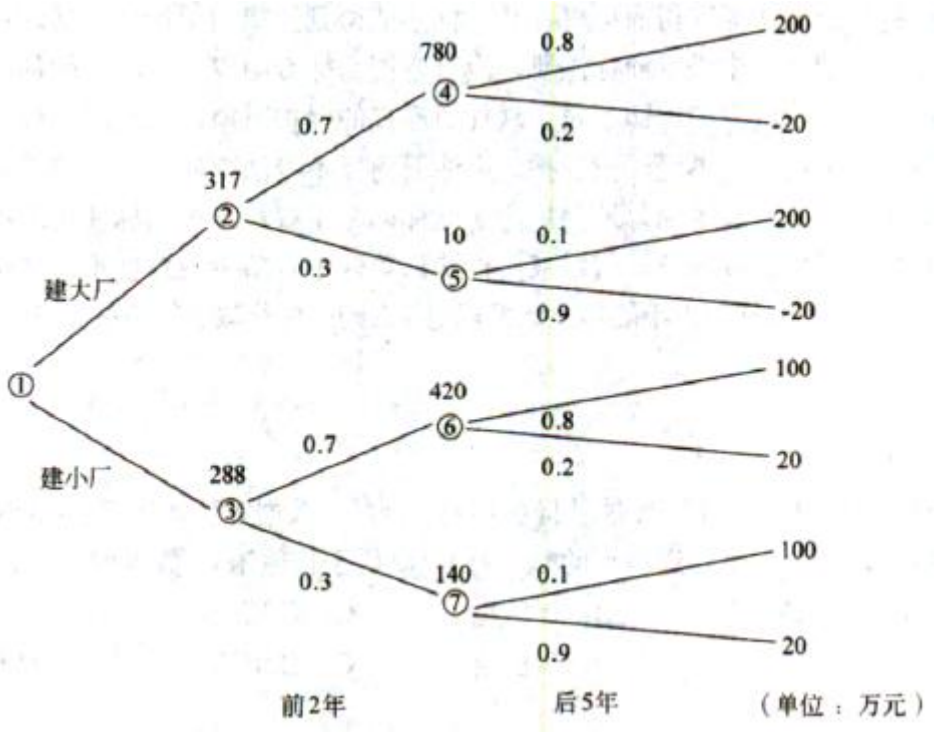
C.建小厂，总收益超 500 万元　　D.建小厂，总收益略多于 300 万元

【答案】B

【解析】本题考查数学应用能力。

采用决策树分析方法解答如下：

先画决策树，从左至右逐步画出各个决策分支，并在各分支上标出概率值，再在最右端分别标出年获利值。然后，从右至左，计算并填写各节点处的期望收益。



在右面四个节点处依次按下列算式计算 5 年的期望值，并将结果分别写在节点处。

节点④：{200*0.8+(-20)*0.2}*5=780

节点⑤：{200*0.1-K-20} *0.9)*5=10

节点⑥：{100*0.8+20*0.2} *5=420

接点⑦：{100*0.1+20*0.9} *5=140

再在②、③节点处按如下算式计算2年的期望值（扣除投资额），并将结果（7年总收益）写在节点处。

节点②:{200*0.7+(-20)*0.3}*2+{780*0.7+10*0.3}-500=317

节点③：{100*0.7+20*0.3}*2+{420*0.7+140*0.3}-200=288

由于节点②处的总收益值大于节点③处的总收益值。因此决定建大厂。

软件商标权的保护对象是指（10）。

(10)A.商业软件　　B.软件商标　　C.软件注册商标　　D.已使用的软件商标

【答案】C

【解析】

软件商标权是软件商标所有人依法对其商标(软件产品专用标识)所享有的专有使用权。在我国，商标权的取得实行的是注册原则，即商标所有人只有依法将自己的商标注册后，商标注册人才能取得商标权，其商标才能得到法律的保护。对其软件产品已经冠以商品专用标识，但未进行商标注册，没有取得商标专用权，此时该软件产品专用标识就不能得到商标法的保护，即不属于软件商标权的保护对象。未注册商标可以自行在商业经营活动中使用，但不受法律保护。未注册商标不受法律保护，不等于对使用未注册商标行为放任自流。为了更好地保护注册商标的专用权和维护商标使用的秩序，需要对未注册商标的使用加以规范。所以《商标法》第四十八条专门对使用未注册商标行为做了规定。未注册商标使用人不能违反此条规定，否则商标行政主管机关将依法予以查处。

基于模拟通信的窄带ISDN能够提供声音、视频、数据等传输服务。ISDN有两种不同类型的信道，其中用于传送信令的是（11），用于传输语音/数据信息的是（12）。

(11)A.信道　　B.B信道　　C.C信道　　D.D信道

(12)A.A信道　　B.B信道　　C.C信道　　D.D信道

【答案】D　B

【解析】

ISDN分为窄带ISDN (Narrowband ISDN, N-ISDN)和宽带ISDN (Broadband ISDN, B-ISDN)。窄带ISDN的目的是以数字系统代替模拟电话系统，把音频、视频和数据业务在一

个网络上统一传输。窄带 ISDN 系统提供两种用户接口：即基本速率接口 2B+D 和基群速率接口 30B+D。其中的 B 信道是 64kb/s 的话音或数据信道，而 D 信道是 16kb/s 或 64kb/s 的信令信道。对于家庭用户，通信公司在用户住所安装一个第一类网络终接设备 NT1。用户可以在连接 NT1 的总线上最多挂接 8 台设备，共享 2B+D 的 144kb/s 信道。大型商业用户则要通过第二类网络终接设备 NT2 连接 ISDN,这种接入方式可以提供 30B+D (2.048Mb/s)的接口速率。

下面关于帧中继的描述中，错误的是（13）。

(13)A.帧中继在第三层建立固定虚电路和交换虚电路

B.帧中继提供面向连接的服务

C.帧中继可以有效地处理突发数据流量

D.帧中继充分地利用了光纤通信和数字网络技术的优势

【答案】A

【解析】

帧中继（Frame Relay, FR)网络运行在 OSI 参考模型的物理层和数据链路层。FR 用第二层协议数据单元帧来承载数据业务，因而第三层被省掉了。帧中继提供面向连接的服务，在互相通信的每对设备之间都存在一条定义好的虚电路，并且指定了一个链路识别码 DLCI。帧中继利用了光纤通信和数字网络技术的优势，FR 帧层操作比 HDLC 简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。所以，帧中继比 X.25 具有更高的传输效率。

海明码是一种纠错编码，一对有效码字之间的海明距离是（14）。如果信息为 10 位，要求纠正 1 位错，按照海明编码规则，需要增加的校验位是（15）位。

(14)A.两个码字的比特数之和　　B.两个码字的比特数之差

C.两个码字之间相同的比特数　　D.两个码字之间不同的比特数

(15)A.3　　B.4　　C.5　　D.6

【答案】D　B

【解析】

海明(Hamming)研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字。码字之间的海明距离是一个码字要变成

另一个码字时必须改变的最小位数。例如，7 位 ASCII 码增加一位奇偶位成为 8 位的码字，这 128 个 8 位的码字之间的海明距离是 2。所以当其中 1 位出错时便能检测出来。两位出错时就变成另外一个有效码字了。

按照海明的理论，纠错编码就是要把所有合法的码字尽量安排在 n 维超立方体的顶点上。使得任一对码字之间的距离尽可能大。如果任意两个码字之间的海明距离是 d，则所有少于等于 d-1 位的错误都可以被检查出来，所有少于 d/2 位的错误都可以被纠正。一个自然的推论是，对某种长度的错误串，要纠正它就要用比仅仅检测它多一倍的冗余位。

如果对于 m 位的数据，增加 k 位冗余位，则组成 n=m+k 位的纠错码。对于 2m 个有效码字中的任意一个，都有 n 个无效但可以纠错的码字。这些可纠错的码字与有效码字的距离是 1，含单个错误位。这样，对于一个有效码字总共有 n+1 个可识别的码字。这 n+1 个码字相对于其他 2m—1 个有效码字的距离都大于 1。这意味着总共有 2m (n+1)个有效的或是可纠错的码字。显然这个数应小于等于码字的所有可能的个数 2n。于是，我们有

$$2^m (n+1) < 2^n$$

因为 n=m+k，我们得出

$$M+k+1 < 2^k$$

对于给定的数据位 m，上式给出了 k 的下界，即要纠正单个错误，k 是必须取的最小值。本题中由于 m=10,所以得到 k=4。

PPP 的认证协议 CHAP 是一种（16）安全认证协议，发起挑战的应该是（17）。

(16)A.一次握手　　B.两次握手　　C.三次握手　　D.同时握手

(17)A.连接方　　B.被连接方　　C.任意一方　　D.第三方

【答案】C　B

【解析】

PPP 支持的质询握手认证协议(Challenge Handshake Authentication Protocol, CHAP)采用三次握手方式周期地验证对方的身份。首先是逻辑链路建立后认证服务器（被连接 方）就要发送一个挑战报文（随机数)，终端计算该报文的 Hash 值并把结果返回服务器。然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较，如果匹配，则认证通 过，连接得以建立，否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与，而密钥是不通过网络传送的，所以 CHAP 是很安全的认证机制。在后续的通信过程中， 每经过一个随机

的间隔，这个认证过程都可能被重复，以缩短入侵者进行持续攻击的时间。值得注意的是，这种方法可以进行双向身份认证，终端也可以向服务器进行挑战， 使得双方都能确认对方身份的合法性。

以下关于无线网络中的直接序列扩频技术的描述中，错误的是（18）。

(18)A.用不同的频率传播信号扩大了通信的范围

B.扩频通信减少了干扰并有利于通信保密

C.每一个信号比特可以用 N 个码片比特来传输

D.信号散布到更宽的频带上降低了信道阻塞的概率

【答案】A

【解析】

在直接序列扩频方案中，信号源中的每一比特用称为码片的 N 个比特来传输，这个过程在扩展器中进行。然后把所有的码片用传统的数字调制器发送出去。在接收端，收到的码片解调后被送到一个相关器，自相关函数的尖峰用于检测发送的比特。好的随机码相关函数具有非常高的尖峰/旁瓣比，如下图所示。数字系统的带宽与其所采用的脉冲信号的持续时间成反比。在 DSSS 系统中，由于发射的码片只占数据比特的 1/N，所以 DSSS 信号的带宽是原来数据带宽的 N 倍。

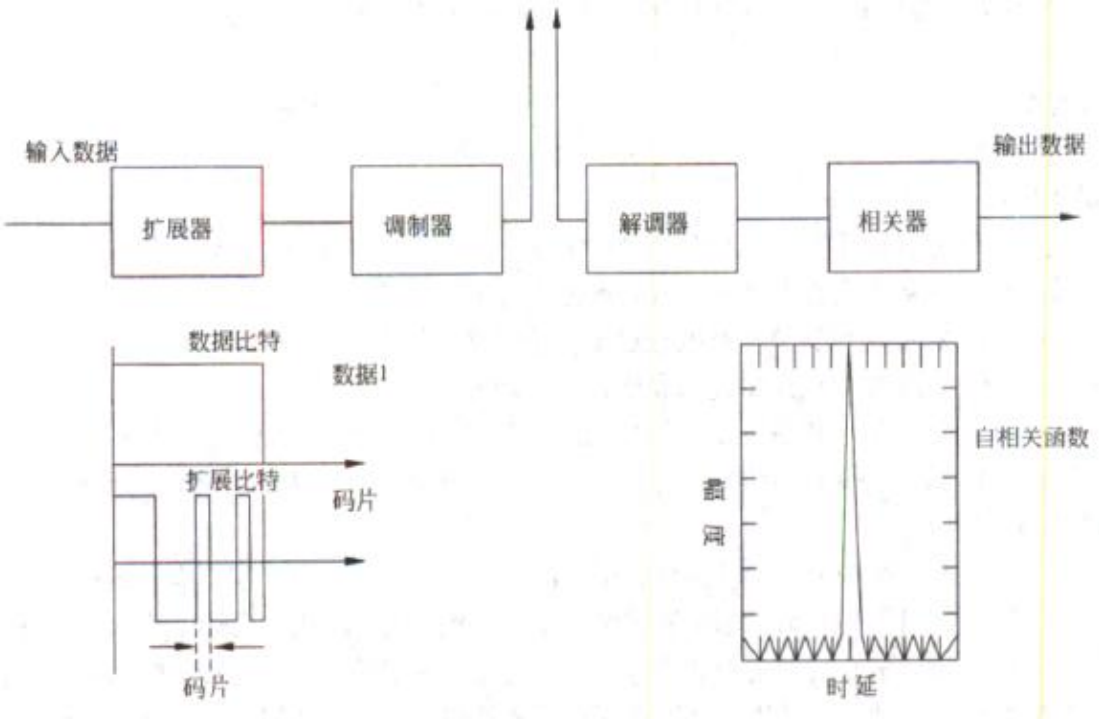


图 DSSS 的频谱扩展器和自相关检测器

在DSSS扩频通信中，每一个信号比特用N个比特的码片来传输，这样使得信号散布到更宽的频带上，降低了信道阻塞的概率，减少了干扰并有利于通信保密。

IEIF定义的集成服务（lntServ）把Internet 服务分成了三种服务质量不同的类型，这三种服务不包括（19）。

(19)A.保证质量的服务：对带宽、时延、抖动和丢包率提供定量的保证

B.尽力而为的服务：这是一般的Internet服务一不保证服务质量

C.负载受控的服务：提供类似于网络欠载时的服务，定性地提供质量保证

D.突发式服务：如果有富余的带宽，网络保证满足服务质量的需求

【答案】D

【解析】

IEIF集成服务（IntServ)工作组根据服务质景的不同，把Internet服务分成了三种类型：

①保证质量的服务（Guranteed Services)：对带宽、时延、抖动和丢包率提供定量的保证；

②负载受控的服务（Controlled-load Services):提供一种类似于网络欠载情况下的服务，这是一种定性的指标；

③尽力而为的服务(Best-Effort):这是Internet提供的一般服务,基本上无任何质量保证。

按照网络分层设计模型，通常把局域网设计为3层，即核心层、汇聚层和接入层，以下关于分层网络功能的搐述中，不正确的是（20）。

(20)A.核心层设备负责数据包过滤、策略路由等功能

B.汇聚层完成路由汇总和协议转换功能

C.接入层应提供一部分管理功能，例如MAC地址认证、计费管理等

D.接入层要负责收集用户信息，例如用户IP地址、MAC地址、访问日志等

【答案】A

【解析】

三层模型将大型局域网划分为核心层、汇聚层和接入层。每一层都有特定的作用。

①核心层是因特网络的高速骨干网，由于其重要性，因此在设计中应该采用冗余组件设计。在设计核心层设备的功能时，应尽量避免使用数据包过滤和策略路由等降低数据包转发速率的功能。如果需要连接因特网和外部网络，核心层还应包括一条或多条连接到外部网络

的连接。

②汇聚层是核心层和接入层之间的分界点，应尽量将资源访问控制、流量的控制等在汇聚层实现。为保证层次化的特性，汇聚层应该向核心层隐藏接入层的细节，例如不管接入层划分了多少个子网，汇聚层向核心层路由器进行路由宣告时，仅宣告由多个子网地址汇聚而成的网络。为保证核心层能够连接运行不同协议的区域网络，各种协议的转换都应在汇聚层完成。

③接入层为用户提供在本地网段访问应用系统的能力，也要为相邻用户之间的互访需求提供足够的带宽。接入层还应该负责一些用户管理功能，以及用户信息的收集工作。

配置路由器有多种方法，一种方法是通过路由器 console 端口连接（21）进行配置，另一种方法是通过 TELNET 协议连接（22）进行配置。

(21)A.中继器　　B.AUX 接口　　C.终端　　D.TCP/IP 网络

(22)A.中继器　　B.AUX 接口　　C.终端　　D.TCP/IP 网络

【答案】C　D

【解析】

对路由器进行初始配置时，要用工作电缆连接仿真终端和路由器的 Console 端口。当路由器部署在网络中时，可以在终端上运行 TELNET 协议，通过 TCP/IP 网络登录到路由器，再在终端上键入配置命令，对路由器进行配置。

如果允许来自子网 172.30.16.0/24 到 172.30.31.0/24 的分组通过路由器，则对应 ACL 语句应该是（23）。

(23)A.access-list 10 permit 172.30.16. 0 255.255. 0.0

B.access-list 10 permit 172.30.16. 0 0.0.255.255

C.access-list 10 permit 172.30.16. 0 0.0.15.255

D.access-list 10 permit 172.30.16. 0 255.255.240.0

【答案】C

【解析】

如果允许来自子网 172.30.16.0/24 到 172.30.31.0/24 的分组通过路由器，则对应的 ACL 语句应该是 access-list 10 permit 172.30.16.0 0.0.15.255。值得注意的是反掩码 0.0.15.255 正好覆盖了 172.30.16.0 网络中最后 12 位表示的全部地址。

结构化布线系统分为六个子系统，其中水平子系统（24）。

(24)A.由各种交叉连接设备以及集线器和交换机等交换设备组成

B.连接干线子系统和工作区子系统

C.由终端设备到信息插座的整个区域组成

D.实现各楼层设备间子系统之间的互连

【答案】B

【解析】

结构化布线系统分为6个子系统：工作区子系统、水平子系统、管理子系统、干线（或垂直）子系统、设备间子系统和建筑群子系统。其中水平子系统是指各个楼层接线间的配线架到工作区信息插座之间所安装的线缆系统，其作用是将干线子系统与用户工作区连接起来。

边界网关协议BGP4被称为路径矢量协议，它传送的路由信息是由一个地址前缀后跟（25）组成。

(25)A.一串IP地址 B.一串自治系统编号 C.一串路由器编号 D.一串子网地址

【答案】B

【解析】

边界网关协议BGP是应用于自治系统（AS)之间的外部网关协议。BGP4基本上是一个距离矢量路由协议，但是与RIP协议采用的算法稍有区别。BGP不但为每个目标计算最小通信费用，而且跟踪通向目标的路径。它不但把目标的通信费用发送给每一个邻居，而且也公告通向目标的最短路径（由地址前缀后跟一串自治系统编号组成)。所以BGP4被称为路径矢量协议。

与RIPv2相比，IGRP协议增加了一些新的特性，以下描述中错误的是（26）。

(26)A.路由度量不再把跳步数作为唯一因素，还包含了带宽、延迟等参数

B.增加了触发更新来加快路由收敛，不必等待更新周期结束再发送更新报文

C.不但支持相等费用通路负载均衡，而且支持不等费用通路的负载均衡

D.最大跳步数由15跳扩大到255跳，可以支持更大的网络

【答案】B

【解析】

内部网关路由协议(Interior Gateway Routing Protocol, IGRP)是 Cisco 公司 1980 年代设计的一种动态距离矢童路由协议。它组合了网络配置的各种因素，包括带宽、延迟、可靠性和负载等作为路由度量。它支持相等费用通路负载均衡和不等费用通路负载均衡。IGRP 的最大跳步数由 15 跳扩大到 255 跳，可以支持比 RIPv2 更大的网络。

默认情况下，IGRP 每 90s 发送一次路由更新广播，在 3 个更新周期内（即 270s）没有从某个路由器接收到更新报文，则宣布该路由不可访问。在 7 个更新周期即 630s 后，IOS 从路由表中清除该路由表项。

用触发更新来加快路由收敛，这是 RlPv2 和 IGRP 都有的功能。

城域以太网在各个用户以太网之间建立多点的第二层连接，IEEE802.1ad 定义的运营商网桥协议提供的基本技术是在以太帧中插入（27）字段，这种技术被称为（28）技术。

(27)A.运营商 VLAN 标记　　B.运营商虚电路标识

C.用户 VLAN 标记　　D.用户帧类型标记

(28)A.Q-in-Q　　B.IP-in-IP　　C.NAT-in-NAT　　D.MAC-in-MAC

【答案】A　A

【解析】

城域以太网论坛（Metro Ethernet Forum, MEF)是由网络设备制造商和网络运营商组成的非盈利组织，专门从事城域以太网的标准化工作。MEF 定义的 E-LAN 服务的基本技术是 802.1q 的 VLAN 帧标记。假定各个用户的以太网称为 C-网，运营商建立的城域以太网称为 S-网。如果不同 C-网中的用户要进行通信，以太帧在进入用户网络接口 (User-Network Interface, UNI)时被插入一个 S-VID (Server Provider-VLAN ID)字段，用于标识 S-网中的传输服务，而用户的 VLAN 帧标记（C-VID)则保持不变，当以太帧到达日标 C-网时，S-VID 字段被删除，如下图所示。这样就解决了两个用户以太网之间透明的数据传输问题。这种技术定义在 IEEE 802.1ad 的运营商网桥协议（Provider Bridge Protocol)中，被称为 Q-in-Q 技术。

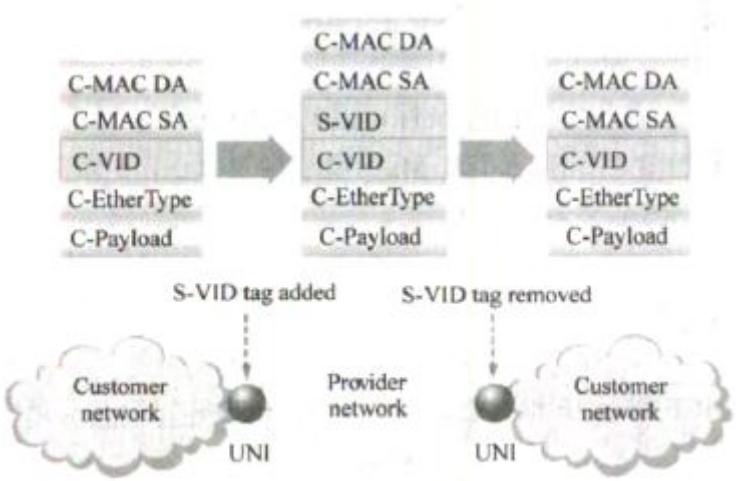


图 802.1ad 的帧格式

Q-in-Q 实际上是把用户 VLAN 嵌套在城域以太网的 VLAN 中传送，由于其简答性和有效性而得到电信运营商的青睐。但是这样一来，所有用户的 MAC 地址在城域以太网中都是可见的，任何 C-网的改变都会影响到 S-网的配置，增加了管理的难度。而且 S-VID 字段只有 12 位，只能标识 4096 个不同的传输服务，网络的可扩展性也受到限制。从用户角度看，网络用户的 MAC 地址都暴露在整个城域以太网中，使得网络的安全性受到威胁。

数据传输时会存在各种时延，路由器在报文转发过程中产生的时延不包括（29）。

(29)A.排队时延　　B.TCP 流控时延　　C.路由计算时延　　D.数据包处理时延

【答案】B

【解析】本题考查路由器的工作原理。

路由器在接收到报文后，先在输入链路进行排队，然后进行检验，计算路由，加入到输出链路进行转发。

某用户为了保障信息的安全，需要对传送的信息进行签名和加密，考虑加解密时的效率与实现的复杂性，加密时合理的算法是（30），签名时合理的算法为（31）。

(30)A.MD5　　B.RC-5　　C.RSA　　D.ECC

(31)A.RSA　　B.SHA-1　　C.3DES　　D.RC-5

【答案】B　A

【解析】本题考查加密和签名算法。

考虑加解密时的效率与实现的复杂性，通常采用对称密钥加密算法对数据进行加密，采

用公钥算法进行签名。SHA-1 和 MD5 属于摘要算法，3DES 和 RC-5 属于对称密钥加密算法，ECC 和 RSA 是公钥算法。

某单位采用 DHCP 进行 IP 地址自动分配，用户收到（32）消息后方可使用其中分配的 IP 地址。

(32)A.DhcpDiscover　　B.DhcpOffer　　C.DhcpNack　　D.DhcpAck

【答案】D

【解析】本题考查 DHCP 协议的工作原理。

当用户初始启动时发送 DhcpDiscover 报文请求 IP 地址；如果有服务器进行响应，发送 DhcpOffer 报文；若用户采用某服务器提供的 IP 地址，采用 DhcpRequest 报文进行请求；服务器在接收到报文后，采用 DhcpAck 报文进行确认，用户收到报文后就可以采用服务器提供的 IP 地址了。

DNS 服务器中提供了多种资源记录，其中（33）定义了域名的反向查询。

(33)A.SOA　　B.NS　　C.PTR　　D.MX

【答案】C

【解析】本题考查 DNS 服务器中的资源记录。

DNS 服务器中提供了多种资源记录，其中类型 SOA 查询的是授权域名服务器；NS 查询的是域名；PTR 是依据 IP 查域名，即域名的反向查询；MX 是邮件服务器记录。

IIS 服务支持多种身份验证，其中（34）提供的安全功能最低。

(34)A..NET Passport 身份验证　　B.集成 Windows 身份验证

C.基本身份验证　　D.摘要式身份验证

【答案】C

【解析】本题考查 IIS 模块中身份验证相关问题。

基本身份验证采用明文形式对用户名和口令进行传送和验证，安全级别最低。

Windows 中的 Netstat 命令显示有关协议的统计信息。下图中显示列表第二列 Local Address 显示的是（35）。当 TCP 连接处于 SYN_SENT 状态时，表示（36）。

```
C:\Documents and Settings\Administrator>netstat -o 1

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1172   121.11.159.208:http    SYN_SENT        1572

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1173   121.11.159.208:http    SYN_SENT        1572

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1173   121.11.159.208:http    SYN_SENT        1572

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    x4ep512rdszwjzp:1176   124.115.3.126:http     ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1178   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1179   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1180   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1182   124.115.3.126:http     ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1183   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1184   124.115.6.52:http      ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1185   222.73.73.173:http     ESTABLISHED     3096
  TCP    x4ep512rdszwjzp:1186   222.73.78.14:http      SYN_SENT        3096
```

(35)A.本地计算机的 IP 地址和端口号　　B.本地计算机的名字和进程 ID

C.本地计算机的名字和端口号　　D.本地计算机的 MAC 地址和进程 ID

(36)A.已经发出了连接请求　　B.连接已经建立

C.处于连接监听状态　　D.等待对方的释放连接响应

【答案】C　A

【解析】本题考查网络管理命令及 TCP 三次握手建立连接状态。

在 Windows 操作系统中，采用命令 Netstat 来显示本机 Internet 应用的统计信息。其中 Local Address 显示的是本地主机的名称及 TCP 连接或 UDP 所采用的端口号。

当 TCP 连接处于 SYN_SENT 状态时，表示已经发出了连接请求，等待对方握手信号；处于连接监听状态是对方被动打开，等待连接建立请求，状态为 LISTEN;连接已经建立状态是 ESTABLISHED;等待对方的释放连接响应状态是 FIN-WAIT-1。

设有下面 4 条路由：210.114.129.0/24、210.114.130.0/24、210.114.132.0/24 和 210.114.133.0/24，如果进行路由汇聚，能覆盖这 4 条路由的地址是（37）。

(37)A.210.114.128.0/21　　B.210.114.128.0/22

C.210.114.130.0/22　　D.210.114.132.0/20

【答案】A

【解析】

展开 IP 地址的第 3 字节如下：

第 1 条路由：10000001

第 2 条路由：10000010

第 3 条路由：10000100

第 4 条路由：10000101

聚合之后该字节前 5 比特网络号，后 3 比特主机号，即网络号 210.114.128.0,掩码长度 21 位。

下面地址中属于单播地址的是（38）。

(38)A.125.221.191.255/18　　B.192.168.24.123/30

C.200.114.207.94/27　　D.224.0.0.23/16

【答案】C

【解析】

下面 4 个网络地址的二进制形式是

(1)125.221.191.255/18　　01111101 .11011101 .10111111.11111111

(2)192.168.24.123/30　　11000000.10101000.00011000.01111011

(3)200.114.207.94/27　　11001000.01110010.11001111.01011110

(4)224.0.0.23/16　　11100000.00000000.00000000.00010111

上面各地址二进制表示中的加黑部分是子网掩码，可以看出 A 和 B 都是广播地址，D 是组播地址，只有 C 是单播主机地址。

IP 地址 202.117.17.255/22 是什么地址？（39）。

(39)A.网络地址　　B.全局广播地址　　C.主机地址　　D.定向广播地址

【答案】C

【解析】

IP 地址 202.117.17.255/22 的二进制形式是 11001010.01110101.00010001.11111111,其中的网络号是 11001010.01110101.000100,主机号是 01.11111111。

IPv6 地址的格式前缀用于表示地址类型或子网地址，例如 60 位的地址前缀 10DE00000000CD3 有多种合法的表示形式，以下选项中，不合法的是（40）。

(40)A.10DE:0000: 0000:CD30: 0000:0000:0000:000/60

B.10DE::CD30:0:0:0:0/60

C.10DE: 0:0:CD3/60

D.10DE: 0:0:CD3::/60

【答案】C

【解析】

以上 IPv6 地址前缀中不合法的是 10DE:0:0:CD3/60，因为这种表示可展开为 10DE:0000:0000:0000:0000:0000:0000:0CD3，另外 CD30 也变成了 0CD3,这些都是错误的。

下列攻击方式中，（41）不是利用 TCP/IP 漏洞发起的攻击。

(41)A.SQL 注入攻击 B.Land 攻击 C.Ping of Deah D.Teardrop 攻击

【答案】A

【解析】本题考查网络安全攻击的基础知识。

SQL 注入攻击是指用户通过提交一段数据库查询代码，根据程序返回的结果，获得攻击者想要的数据，这就是所谓的 SQL Injection,即 SQL 注入攻击。这种攻击方式是通过对数据库查询代码和返回结果的分析而实现的。

Land 攻击是指攻击者将一个包的源地址和目的地址都设置为目标主机的地址，然后将该包通过 IP 欺骗的方式发送给被攻击主机，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度地降低了系统性能。

Ping of Death 攻击是攻击者向被攻击者发送一个超过 65536 字节的数据包 ping 包，由于接收者无法处理这么大的 ping 包而造成被攻击者系统崩溃、挂机或重启。

Teardrop 攻击就是利用 IP 包的分段/重组技术在系统实现中的一个错误，即在组装 IP 包时只检查了每段数据是否过长，而没有检查包中有效数据的长度是否过小，当数据包中有效数据长度为负值时，系统会分配一个巨大的存储空间，这样的分配会导致系统资源大量消耗，直至重新启动。

通过以上解释，可见，Land 攻击、Ping of Death 攻击和 Teardrop 攻击均是利用 TCP/IP 的漏洞所发起的攻击。

下列安全协议中（42）是应用层安全协议。

(42)A.IPSec B.L2TP C.PAP D.HTTPS

【答案】D

【解析】本题考查网络安全协议的基础知识。

IPSec 是 IETF 制定的 IP 层加密协议，PKJ 技术为其提供了加密和认证过程的密钥管理功能。IPSec 主要用于开发新一代的 VPN。

L2TP 是一种二层协议主要是对传统拨号协议 PPP 的扩展，通过定义多协议跨越第二层点对点链接的一个封装机制，来整合多协议拨号服务至现有的因特网服务提供商点，保证分散的远程客户端通过隧道方式经由 Internet 等网络访问企业内部网络。

PAP 协议是二层协议 PPP 协议的一种握手协议，以保证 PPP 链接安全性。

HTTPS 是一个安全通信通道，用于在客户计算机和服务器之间交换信息。它使用安全套接字层（SSL)进行信息交换，所有的数据在传输过程中都是加密的。

某网络管理员在园区网规划时，在防火墙上启用了 NAT，以下说法中错误的是（43）.

(43)A.NAT 为园区网内用户提供地址翻译和转换，以使其可以访问互联网

B.NAT 为 DMZ 区的应用服务器提供动态的地址翻译和转换，使其能访问外网

C.NAT 可以隐藏内部网络结构以保护内部网络安全

D.NAT 支持一对多和多对多的地址翻译和转换

【答案】B

【解析】本题考查防火墙功能的知识。

NAT (Network Address Translation)叫做网络地址翻译，或者网络地址转换，它的主要功能是对使用私有地址内部网络用户提供 Internet 接入的方式，将私有地址固定地转换为公有地址以访问互联网，NAT 支持一对多和多对多的地址转换方式。由于通过 NAT 访问互联网的用户经过了地址翻译/转换，并非使用原地址访问互联网，因此外部网络对内网的地址结构是不得而知的，依此形成了对内部网络的隐藏和保护。

不能对内部网络中服务器使用 NAT 进行地址转换或者地址翻译，否则，用户将无法联系到内部网络的服务器。

在 SET 协议中，默认使用（44）对称加密算法。

(44)A.IDEA B.RC5 C.三重 DES D.DES

【答案】D

【解析】本题考查安全支付协议的知识。

SET 协议是 PKI 框架下的一个典型实现。安全核心技术主要有公开密钥加密、数字签名、数字信封、消息摘要、数字证书等，主要应用于 B2C 模式中保障支付信息的安全性。SET 协议使用密码技术来保障交易的安全，主要包括散列函数、对称加密算法和非对称加密算法等。SET 中默认使用的散列函数是 SHA，对称密码算法则通常采用 DES，公钥密码算法一般采用 RSA。

2013 年 6 月，WiFi 联盟正式发布 IEEE 802.11ac 无线标准认证。802.11ac 是 802.11n 的继承者，新标准的理论传输速度最高可达到 1Gbps。它采用并扩展了源自 802.11n 的空中接口概念，其中包括：更宽的 RF 带宽，最高可提升至（45）；更多的 MIMO 空间流，最多增加到（46）个；多用户的 MIMO，以及更高阶的调制，最大达到（47）。

(45)A.40MHz　　B.80MHz　　C.160MHz　　D.240MHz

(46)A.2　　B.4　　C.8　　D.16

(47)A.16QAM　　B.64QAM　　C.128QAM　　D.256QAM

【答案】C　C　D

【解析】本题考查新的 802.11ac 无线标准认证。

IEEE 802.11ac，是一个 802.11 无线局域网(WLAN)通信标准，它通过 5GHz 频带（也是其得名原因）进行通信。理论上，它能够提供最少 1Gbps 带宽进行多站式无线局域网通信，或是最少 500Mbps 的单一连接传输带宽。802.11ac 是 802.11n 的继承者。它采用并扩展了源自 802.11n 的空中接口(air interface) 概念，包括：更宽的 RF 带宽（提升至 160MHz），更多的 MIMO 空间流（spatial streams) (增加到 8)，多用户的 MIMO，以及更高阶的调制(modulation)(达到 256QAM)。

RAID 系统有不同的级别，如果一个单位的管理系统既有大量数据需要存取，又对数据安全性要求严格，那么此时应采用（48）。

(48)A.RAID 0　　B.RAID 1　　C.RAID 5　　D.RAID 0+1

【答案】D

【解析】本题考查 RAID 的基本功能和应用。

独立硬盘冗余阵列（RAID, Redundant Array of Independent Disks)，旧称廉价磁盘

冗余阵列（Redundant Array of Inexpensive Disks)，简称硬盘阵列。其基本思想就是把多个相对便宜的硬盘组合起来，成为一个硬盘阵列组，使性能达到甚至超过一个价格昂贵、容量巨大的硬盘。根据选择的版本不同，RAID 比单颗硬盘有以下一个或多个方面的好处：增强数据集成度，增强容错功能，增加处理量或容量。另外，磁盘阵列对于电脑来说，看起来就像一个单独的硬盘或逻辑存储单元，分为 RAID-0、RAID-1 RAID-1E、 RAID-5、RAID-6、RAID-7、RAID-10、RAID-50、RAID-60。

①RAID0:它将两个以上的磁盘串联起来，成为一个大容量的磁盘。在存放数据时，分段后分散存储在这些磁盘中，因为读写时都可以并行处理，所以在所有的级别中，RAID 0 的速度是最快的。但是 RAID 0 既没有冗余功能，也不具备容错能力，如果一个磁盘（物理）损坏，所有数据都会丢失。

②RAID1:将两组以上的 N 个磁盘相互作镜像,在一些多线程操作系统中能有很好的读取速度，理论上读取速度等于硬盘数量的倍数，另外写入速度有微小的降低。只要一个磁盘正常即可维持运作，可靠性最高。

③RAID5:这是一种储存性能、数据安全和存储成本兼顾的存储解决方案。它使用的是 Disk Striping（硬盘分区）技术。RAID 5 至少需要三颗硬盘，RAID 5 不是对存储的数据进行备份，而是把数据和相对应的奇偶校验信息存储到组成 RAID5 的各个磁盘上，并且奇偶校验信息和相对应的数据分别存储于不同的磁盘上。当 RAID5 的一个磁盘数据发生损坏后，可以利用剩下的数据和相应的奇偶校验信息去恢复被损坏的数据。RAID5 可以理解为是 RAID 0 和 RAID 1 的折衷方案。

④RAID0+1:这是 RAID 0 和 RAID 1 的组合形式，也称为 RAID 01。该方案是存储性能和数据安全兼顾的方案。它在提供与 RAID 1 一样的数据安全保障的同时，也提供了与 RAID 0 近似的存储性能。

采用 ECC 内存技术,一个 8 位的数据产生的 ECC 码要占用 5 位的空间,一个 32 位的数据产生的 ECC 码要占用__（49）__位的空间。

(49)A.5　　B.7　　C.20　　D.32

【答案】B

【解析】本题考查服务器技术的相关概念。

ECC (Error Checking and Correcting,错误检查和纠正）不是一种内存类型，只是一种内存技术。ECC 纠错技术也需要额外的空间来储存校正码，但其占用的位数跟数据的长度

并非成线性关系。

ECC 码将信息进行 8 比特位的编码，采用这种方式可以恢复 1 比特的错误。每一次数据写入内存的时候，ECC 码使用一种特殊的算法对数据进行计算，其结果称为校验位 (Check Bits)。然后将所有校验位加在一起的和是“校验和”(checksum)，校验和与数据一起存放。当这些数据从内存中读出时，采用同一算法再次计算校验和，并和前面的计算结果相比较，如果结果相同，说明数据是正确的，反之说明有错误，ECC 可以从逻辑上分离错误并通知系统。当只出现单比特错误的时候，ECC 可以把错误改正过来不影响系统运行。

一个 8 位的数据产生的 ECC 码要占用 5 位的空间，16 位数据需占用 6 位；而 32 位的数据则只需再在原来基础增加一位，即 7 位的 ECC 码即可，以此类推。

在微软 64 位 Windows Server 2008 中集成的服务器虚拟化软件是（50）。

(50)A.ESX Server　　B.Hyper-V　　C.XenServer　　D.Vserver

【答案】B

【解析】本题考查服务器技术的相关概念。

虚拟化打破了底层设备、操作系统、应用程序，以及用户界面之间牢同绑定的纽带，彼此之间不再需要紧密耦合，从而可以变成可以按需递交的服务。最终可以实现这样的目标：在任何时间、任何地方，任何用户可以访问任何应用程序，都可以获得任何所需的用户体验。选项中 ESX Server 是由 VMware 开发的 VMware ESX Server 服务器，该服务器在通用环境下分区和粮合系统的虚拟主机软件。

Hyper-V 是由 Windws Server 2008 中集成的服务器虚拟化软件，其采用微内核架构，兼顾了安全性和性能的要求。

XenServer 是思杰基于 Linux 的虚拟化服务器，是一种全面而易于管理的服务器虚拟化平台，基于 Xen Hypervisor 程序之上。

Vserver 是服务器虚拟化软件，可在一台物理服务器上创建多个虚拟机，每个虚拟机相互独立，相互隔离，且像物理机一样拥有自己的 CPU、内存、磁盘和网卡等资源，从而实现物理服务器的虚拟化，同时运行多个业务系统而互不影响。

跟网络规划与设计生命周期类似，网络故障的排除也有一定的顺序。在定位故障之后，合理的故障排除步骤为（51）。

(51)A.搜集故障信息、分析故障原因、制定排除计划、实施排除行为、观察效果

B.观察效果、分析故障原因、搜集故障信息、制定排除计划、实施排除行为

C.分析故障原因、观察效果、搜集故障信息、实施排除行为、制定排除计划

D.搜集故障信息 、观察效果、分析故障原因、制定排除计划、实施排除行为

【答案】A

【解析】本题考查故障排除流程。

网络故障的排除先需定位故障，分析故障原因，然后制定排除计划，实施排除行为，观察效果。

组织和协调是生命周期中保障各个环节顺利实施并进行进度控制的必要手段,其主要实施方式为（52）。

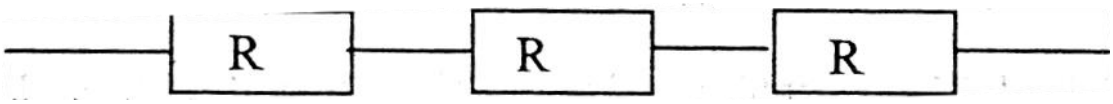
(52)A.技术审查 B.会议 C.激励 D.验收

【答案】B

【解析】本题考查生命周期相关阶段任务。

组织和协调是进度控制的必要手段，通常采用会议形式进行。

三个可靠度 R 均为 0.9 的部件串联构成一个系统，如下图所示：



则该系统的可靠度（53）。

(53)A.0.810 B.0.729 C.0.900 D.0.992

【答案】B

【解析】本题考查系统可靠度。

由于串联，故可靠度为 0.9*0.9*0.9=0.729。

在下列业务类型中，上行数据流量远大于下行数据流量的是（54）。

(54)A.P2P B.网页浏览 C.即时通信 D.网络管理

【答案】D

【解析】本题考查网络应用的基本知识。

P2P 是 Peer-to-Peer 的缩写。P2P 网中所有参与系统的结点处于完全对等的地位，即在覆盖网络中的每一个结点都同时扮演着服务器和客户端两种角色,每个在接受来自其他结点

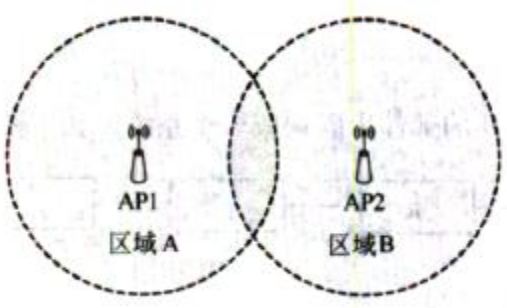
的服务同时，也向其他结点提供服务。因此，这类网络业务，上行数据流了与下行数据流量基本相同。

网页浏览是目前互联网上应用最为广泛的一种服务，该服务的运行是基于 B/S 结构的，即用户通过浏览器向服务器发送一个网页请求，服务器再将该网页数据返回给用户，这种模式下，下行数据流量将远大于上行数据流量。

即时通信是使用相应的即时通信软件实现用户之间实时通信和交流的一种互联网服务。在该服务中，用户在发送数据的同时也在接收数据，双向数据流量基本相同。

网络管理是网络管理员通过 SNMP 协议对网络设备发送大景管理命令和管理信息，而对于命令的接收者并无或者极少的信息反馈给管理端，在这种业务中，上行流量远远大于下行数据流量。

企业无线网络规划的拓扑图如下所示，使用无线协议是 802.11b/g/n，根据 IEEE 规定，如果 AP1 使用 1 号信道，AP2 可使用的信道有 2 个，是（55）。



(55)A.2 和 3　　B.11 和 12　　C.6 和 11　　D.7 和 12

【答案】C

【解析】本题考查无线网络的基本知识。

2.4GHz 无线网络信道划分是按照每 5MHz 一个信道划分，每个信道 22MHz，将 2.4GHz 频段划分出 13 个信道，而这 13 个信道中有相互覆盖和相互重叠的情况，为了无线网络能够互不干扰的工作，在 13 个信道中，只有 3 个信道可用，1、6、11 号信道。

目前大部分光缆工程测试都采用 OTDR（光时域反射计）进行光纤衰减的测试，OTDR 通过检测来自光纤的背向散射光进行测试。这种情况下采用（56）方法比较合适。

(56)A.双向测试　　B.单向测试　　C.环形测试　　D.水平测试

【答案】A

【解析】本题考查利用OTDR（光时域反射计）进行光缆测试的方法。

目前大部分工程测试都采用OTDR（光时域反射计）来进行光纤衰减的测试的，而OTDR是通过测试来自光纤的背向散射光实现测试的。这样，因为两个方向的散射光往往是不同的，从而导致两个方向测试的结果不同。严格地说，两个方向测试结果都与实际衰减值不同。将两个方向的测试结果取代数和，再除2（这个方法也适合接头衰减的测试）的结果比较接近实际指标，因此就规定双向测试方法。

以下关于网络规划需求分析的描述中，错误的是（57）。

(57)A.对于一个新建的网络，网络工程的需求分析不应与软件需求分析同步进行

B.在业务需求收集环节，主要需要与决策者和信息提供者进行沟通

C.确定网络预算投资时，需将一次性投资和周期性投资均考虑在内

D.对于普通用户的调查，最好使用设计好的问卷形式进行

【答案】A

【解析】本题考查网络规划需求分析的基本知识。

在整个网络开发过程中，业务需求调查是理解业务本质的关键，应尽量保证设计的网络能够满足业务的需求，在业务需求收集和调查环节，设计人员须同企业或者部门的领导者进行充分的沟通，已确定网络建设各个方面的需求和问题。

一般在进行网络工程的需求分析时，同时将软件需求分析同步进行，因为网络工程的实施和包括对于网络系统中所使用的软件的安装和调试等环节。

网络预算一般分为一次性投资预算和周期性投资预算，一般来说年度发生的周期性投资预算和一次性投资预算之间的比例为10%～15%是比较合理的。一次性投资预算主要用于网络的初始建设，包括设备采购、购买软件、维护和测试系统，培训工作人员以及设计和安装系统的费用等；应根据一次性投资预算，对设备、软件进行选型，对培训工作量进行限定，确保网络初始建设的可行性。周期性投资预算主要用于后期的运营维护，包括人员消耗、设备维护消耗、软件系统升级消耗、材料消耗、信息费用、线路租用费用等多个方面；同时，对客户单位的网络工作人员的能力进行分析，考察他们的工作能力和专业知识是否能够胜任以后的工作，并提出相应的建议，是评判周期性投资预算是否能够满足运营需要的关键之一。对于普通用户的调查过程一般采用问卷调查的方式进行，这种方式能够更好地提高调查的效率和调查结果的可用性。

在局域网中，划分广播域的边界是（58）。

(58)A.HUB　　B.Modem　　C.VLAN　　D.交换机

【答案】C

【解析】本题考查网络设备的基本知识。

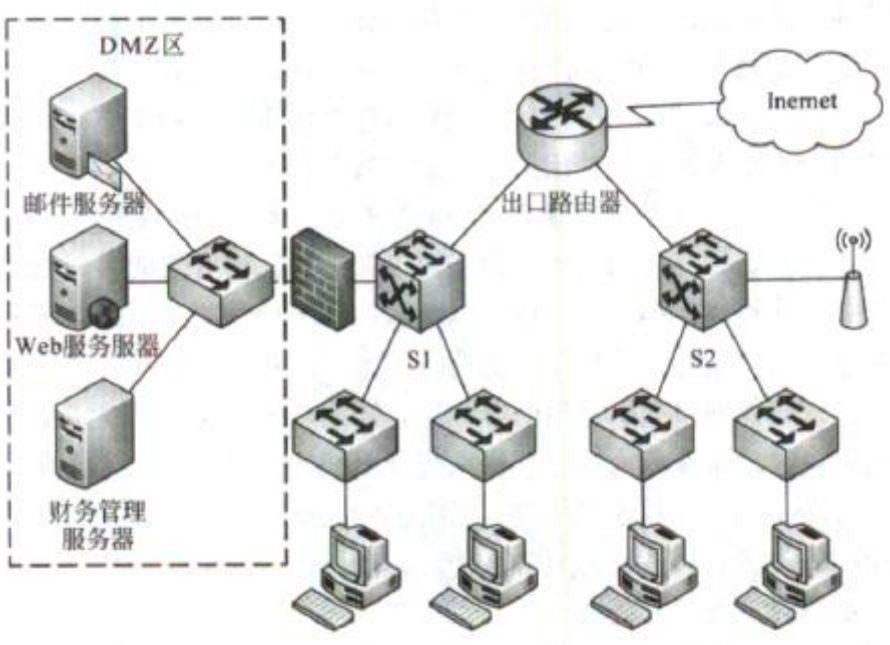
HUB 也叫集线器，是一种总线型的网络连接设备，工作于 OSI 模型的物理层，使用集线器所连接的网络拓扑为总线型网络，它是一个广播域，同时也是冲突域。

Modem 是调制解调器，主要为实现在传统模拟线路上传输数字信号的一种设备。

VLAN 是-种通过逻辑地在交换机上根据一定的规则分隔广播数据包的方式，通过为进入交换机的数据帧标记不同的 vlan tag,只有带有与接口相同的 vlan tag 的数据帧才能够被转发和通信。

交换机在默认情况下，所有的接口均处于同一个广播域中，因此它不具备划分广播域边界的功能。

工程师为某公司设计了如下网络方案。



下面关于该网络结构设计的叙述中，正确的是（59）。

(59)A.该网络采用三层结构设计，扩展性强

B.S1、S2 两台交换机为用户提供向上的冗余连接，可靠性强

C.接入层交换机没有向上的冗余连接，可靠性较差

D.出口采用单运营商连接，带宽不够

【答案】C

【解析】本题考查网络设计部署的基本知识。

根据图示的拓扑链接可见，该网络规划采用的是两层结构的扁平化设计方式，而两台核心层交换机 S1、S2 之间并未提供冗余连接，这样的连接方式，会造成很严重的单点故障，因此不能为整个网络提供较高的可靠性。Internet 接入采用单运营商接入的方式，并不能够导致带宽不够的问题，而接入层向核心层并未提供冗余连接，网络的可靠性较差。

下面关于防火墙部分连接的叙述中，错误的是（60）。

(60)A.防火墙应与出口路由器连接　　B.Web 服务器连接位置恰当合理

C.邮件服务器连接位置恰当合理　　D.财务管理服务器连接位置恰当合理

【答案】D

【解析】本题考查网络服务器部署的基本知识。

网络中的防火墙位置可放置于接入互联网的路由器之前，也可将其放置于网络的核心层，以提高内部网络用户的使用体验，在防火墙的 DMZ 区中，所放置的可以是为内部网络用户或者外部网络用户提供服务的各类服务器，而财务管理服务器不属子公共服务器，应放置于专用网络中。

下面关于用户访问部分的叙述中，正确的是（61）。

(61)A.无线接入点与 S2 相连，可提高 WLAN 用户的访问速率

B.有线用户以相同的代价访问 Internet 和服务器，设计恰当合理

C.可增加接入层交换机向上的冗余连接，提高有线用户访问的可靠性

D.无线接入点应放置于接入层，以提高整个网络的安全性

【答案】D

【解析】本题考查接入层网络部署的基本知识。

网络接入层的作用是为用户提供接入到网络的接口，无线网络接入点为无线用户提供网络的接入，一般的部署方式是将无线网络接入点放置于网络接入层设备，题（59）的图的设计中，将无线接入点与核心层设备 S2 相连是不合理的。由于核心层设备为采用冗余连接，因此两端的用户在访问内部服务器时的代价是不同的，同时，即使在接入层添加到核心层的冗余连接，也并不能提高有线网络用户访问内部网络的可靠性，因此该项设计不恰当。

下列对于网络测试的叙述中，正确的是（62）。

(62)A.对于网络连通性测试，测试路径无需覆盖测试抽样中的所有子网和 VLAN

B.对于链路传输速率的测试，需测试所有链路

C.端到端链路无需进行网络吞吐量的测试

D.对于网络系统延时的测试，应对测试抽样进行多次测试后取平均值，双向延时应≤1ms

【答案】D

【解析】本题考查网络测试的基本知识。

对新建网络进行测试时，无需对链路传输速率、端到端测试和所有子网和 VLAN 进行测试，一般采取抽样测试的方式进行，测试需对所有抽样进行测试，以提高测试的准确性；对于端到端链路测试中，吞吐量的测试是其中一项非常重要的测试项目。

下列地址中，（63）是 MAC 组播地址。

(63)A.0x0000.5E2F.FFFF　　B.0x0100.5E4F.FFFF

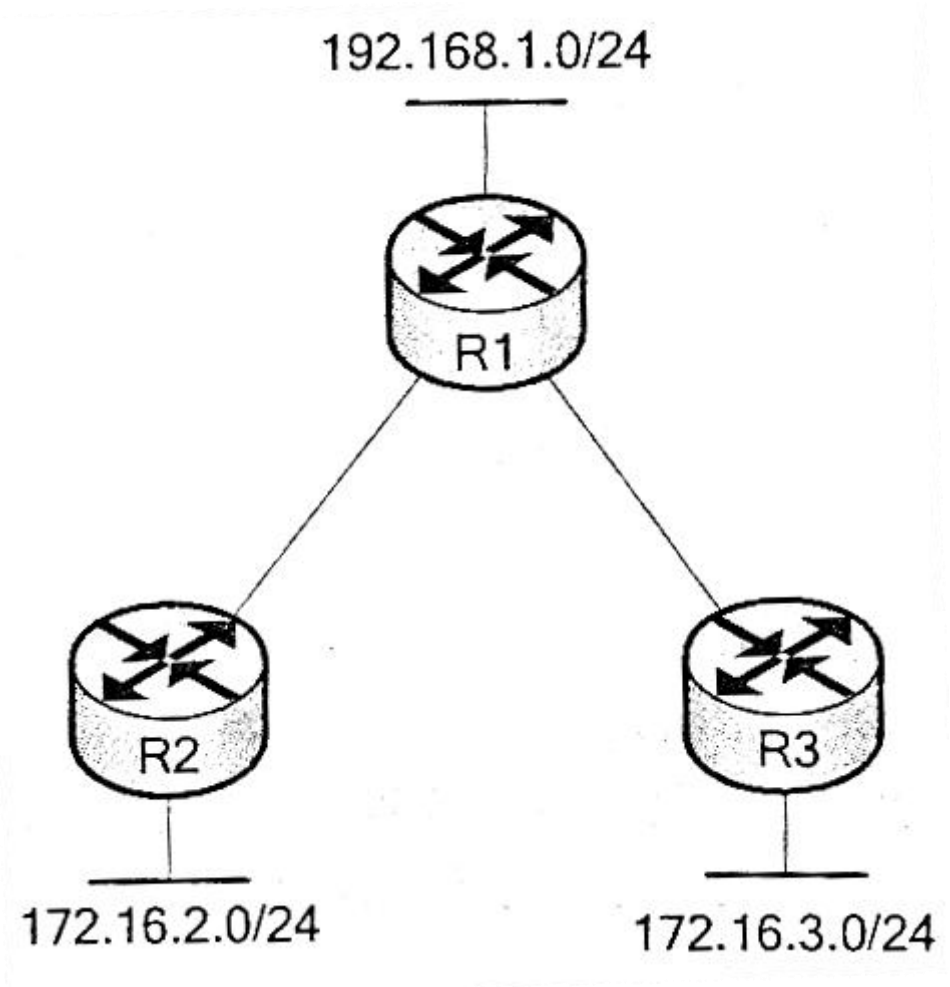
C.0x0200.5E6F.FFFF　　D.0x0300.5E8F.FFFF

【答案】B

【解析】本题考查网络地址的基本知识。

MAC (Media Access Control)地址，或称为 MAC 地址、硬件地址，用来定义网络设备的位置。采用十六进制数表示，共六个字节（48 位）。其中，前三个字节是由 IEEE 的注册管理机构 RA 负责给不同厂家分配的代码（高位 24 位），也称为“编制上唯一的标识符’’（Organizationally Unique Identifier)，后三个字节（低位 24 位）由各厂家自行指派给生产的适配器接口，称为扩展标识符（唯一性)。一个地址块可以生成 224 个不同的地址。MAC 地址中有一部分保留地址用于组播，范围是 0100.5E00.0000——0100.5E07.FFFF。

某网络拓扑图如下所示，三台路由器上均运行 RIPv1 协议，路由协议配置完成后，测试发现从 R1 ping R2 或者 R3 的局域网，均有 50%的丢包，出现该故障的原因可能是（64）。



(64)A.R1 与 R2、R3 的物理链路连接不稳定

B.R1 未能完整的学习到 R2 和 R3 的局域网路由

C.管理员手工地对 R2 和 R3 进行了路由汇总

D.RIP 协议版本配置错误，RIPv1 不支持不连续子网

【答案】D

【解析】本题考查网络路由协议的基本知识。

三台路由器运行 RIPv1 协议，从 R1 pingR2 或者 R3 的局域网，出现均有 50%的丢包现象，RIPv1 不支持不连续的子网，因此，在 R1 上针对 R2 和 R3 局域网的 172.16.2.0/24 和 172.16.3.0/24 路由进行了路由汇总，统一汇总成 172.16.0.0/16 路由，因此，当从 R1 ping R2 或者 R3 时，路由器认为从 R1 与 R2 和 R3 相连的接口均可到达，实现了不恰当的负 载均衡。

使用长度 1518 字节的帧测试网络吞吐量时，1000M 以太网抽样测试平均值是（65）时，该网络设计是合理的。

(65)A.99% B.80% C.60% D.40%

【答案】A

【解析】本题考查网络测试的基本知识。

吞吐率是指空载网络在没有丢包的情况下，被测网络链路所能达到的最大数据包转发速率。吞吐率测试需按照不同的帧长度（包括 64、128、256、512、1024、1280、1518 字节）分别进行测量。系统在帧长度为 1518 字节测试 1000M 以太网时，测试平均值应为 99%时，网络设计达到要求。

某企业内部两栋楼之间距离为 350 米，使用 62.5/125μm 多模光纤连接。100Base-FX 连接一切正常，但是该企业将网络升级为 1000Base-FX 后，两栋楼之间的交换机无法连接。经测试，网络链路完全正常，解决此问题的方案是（66）。

(66)A.把两栋楼之间的交换机模块更换为单模模块

B.把两栋楼之间的交换机设备更换为路由器设备

C.把两栋楼之间的多模光纤更换为 50/125μm 多模光纤

D.把两栋楼之间的多模光纤更换为 8/125μm 单模光纤

【答案】C

【解析】本题考查网络故障解决方法。

两栋楼距离 350 米，使用多模光纤连接，由 100Base-FX 升级至 1000Base-SX 后无法连通。根据光纤传输知识可知，1000BASE-SX 所使用的光纤有：波长为 850nm，分为 62.5/125μm 多模光纤、50/125μm 多模光纤。其中使用 62.5/125μm 多模光纤的最大传输距离为 220m，使用 50/125μm 多模光纤的域大传输距离为 500 米。因此只需要将两栋楼之间的多模光纤更换为 50/125μm 多模光纤即可。

IANA 在可聚合全球单播地址范围内指定了一个格式前缀来表示 IPv6 的 6to4 地址，该前缀为（67）。

(67)A.0x1001 B.0x1002 C.0x2002 D.0x2001

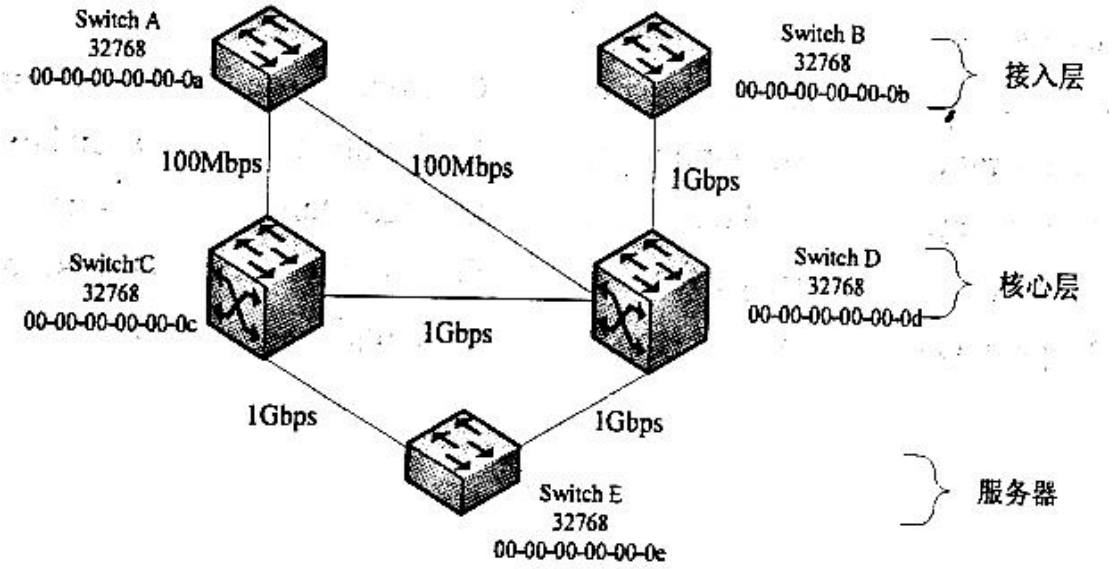
【答案】C

【解析】本题考查可聚合全球单播地址的知识。

6to4 隧道采用特殊的 IPv6 地址。IANA（因特网编号分配委员会）为 6to4 隧道方式地分配了一个永久性的 IPv6 格式前缀 0x2002，表示成 IPv6 地址前缀格式为 2002::/16。如果

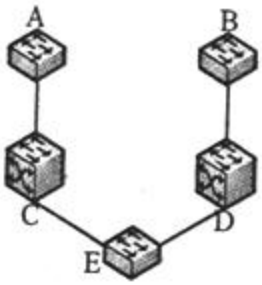
一个用户站点拥有至少一个有效的全球唯一的 32 位 IPv4 地址（V4ADDR)，那么该用户站点将不需要任何分配申请即可拥有如下的 IPv6 地址前缀 2002:(v4ADDR)::/48。

下图所示是一个园区网的一部分，交换机 A 和 B 是两台接入层设备，交换机 C 和 D 组成核心层，交换机 E 将服务器群连接至核心层。如图所示，如果采用默认的 STP 设置和默认的选举过程，其生成树的最终结果为（68）。

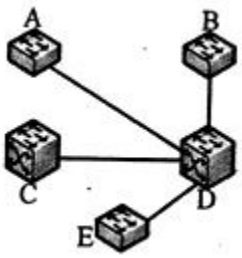


这时交换机 B 上的一台工作站要访问园区网交换机 E 上的服务器其路径为(69).由此可以看出，由此可以看出，如果根网桥的选举采用默认配置，下列说法中不正确的是（70） 。

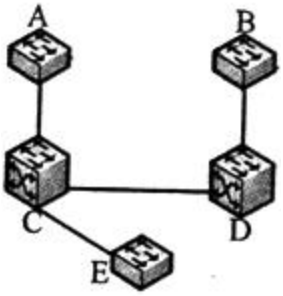
(68)A.



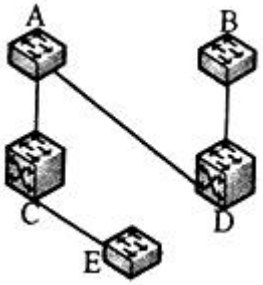
B.



C.



D.



(69)A.B-D-E B.B-D-C-E C.B-D-A-C-E D.不能抵达

(70)A.最慢的交换机有可能被选为根网桥

B.有可能生成低效的生成树结构

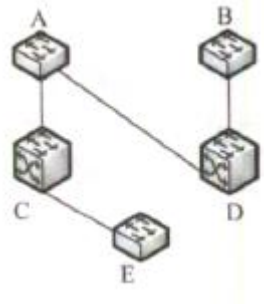
C.只能选择一个根网桥，没有备用根网桥

D.性能最优的交换机将被选为根网桥

【答案】D C D

【解析】本题考查STP相关知识。

如图所示，在默认STP设置下，接入层交换机A将成为根网桥，因为它的MAC地址域小，而所有交换机的优先级都一样。这样交换机A被选作根后，它就不能使用1Gbps 的链路，它只有两条100Mbps的链路。根据默认的选举过程，删除处于阻断状态的链路后的网络，从中可以看出生成树的最终结果（如下图所示)。接入交换机A是根交换机，在交换机B上的工作站必须通过核心层（交换机D)、接入层（交换机A)和核心层（交换机C)，才能最后到达交换机E上的服务器，显然这种行为是低效的。STP可以自动地使用默认设置和默认选举过程，但得到的树结构可能与预期的截然不同。



There are two general approaches to attacking a (71)encryption scheme.The first attack is known as cryptanalysis.Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the (72) or even some sample plaintext-ciphertext pairs. This type of (73) exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used. If the attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised. The second method, known as the (74)-force attack, is to try every possible key on a piece of (75) until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

(71)A.stream B.symmetric C.asymmetric D.advanced

(72)A.operation	B.publication	C.plaintext	D.ciphertext
(73)A.message	B.knowledge	C.algorithm	D.attack
(74)A.brute	B.perfect	C.atribute	D.research
(75)A.plaintext	B.ciphertext	C.sample	D.code

【答案】B C D A B

【解析】

有两种常用的方法可以攻击对称密钥加密方案。第一种攻击叫做密码分析学。密码分析攻击依赖于算法的特性，也许还要加上某些有关明文的一般性特征的知识，甚至需要某些明文-密文对的样品作为辅助。这种类型的攻击利用了算法的特点，企图推导出特殊的明文或者推导出当前使用的密钥。如果这种攻击成功地导出了密钥，其效果将是灾难性的：所有将来和过去用这个密钥加密的报文都会被突破。第二种方法叫做蛮力攻击，就是用每一种可能的密钥在一段密文上进行试验，直到将其转换为可理解的明文。平均来说，要达到成功需要试验的密钥数量为各种可能的密钥数量的一半。

试题一（共 25 分）

阅读下列说明，回答问题 1 至问题 5,将解答填入答题纸的对应栏内。

某高校拟对学生公寓网络（已知网络主机超过 3000 台）进行改造，该校网络部门在技术方案讨论的过程中，提出了以太接入、ADSL 接入和 GPON 接入三种思路。该部门技术主管在对三种方案的建设成本、网络安全、系统容易维护、宽带综合业务等方面综合考虑后决定才用 GPON 接入方式，并给出基于 GPON 技术的学生公寓宽带初步设计方案，如图 1-1 所示。

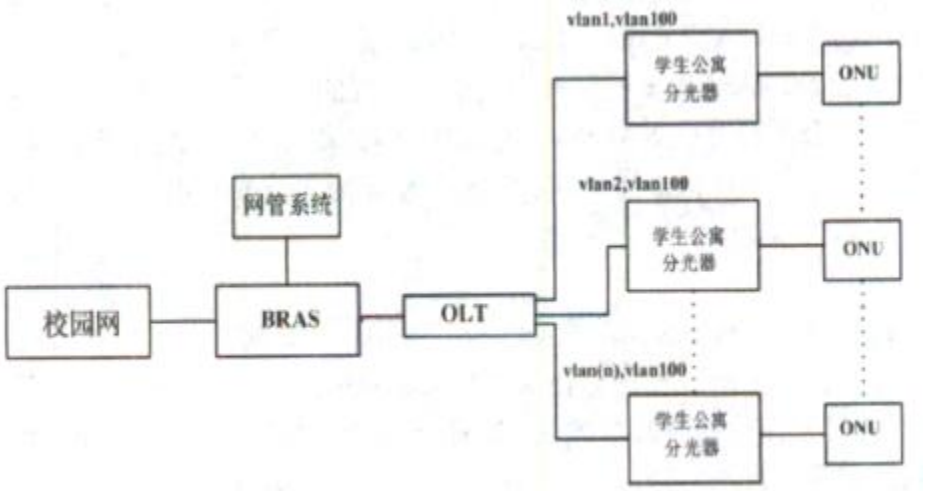


图 1-1

【问题 1】

请比较以太接入、ADSL 接入和 GPON 接入三种方式的特点，并简要说明选择 GPON 接入方式的理由。

【参考答案】

方　案	特　点
以太网接入	传统局域网采用的组网方式、成本低、多种介质
ADSL 接入	通过电话线就可实现高速网络接入
GPON 接入	成本低、维护简单、高带宽、抗干扰

理由：GPON 是由局端设备 OLT 与多个用户端设备 ONU 之间通过无源光分配网 ODN 连接的光接入网络。“无源”的特性使得成本低、维护简单，可提供千兆级带宽，并且技术成熟、抗干扰，已经逐渐成为当今主流的网络接入方式（三网合一与 FTTH 接入）。

【试题分析】

本题考查网络接入技术以及局域网配置、产品主要性能指标等相关知识即应用。

无源光纤网络 PON (Passive optical network)又称被动式光纤网络，是光纤通信网络的一种，其特色为不用电源就可以完成信号处理，除了终端设备需要用到电以外，其中间的

节点则以精致小巧的光纤元件构成。PON 系统结构主要由中心局的光线路终端 (OLT)、包含无源光器件的光分配网（ODN)、用户端的光网络单元/光网络终端 (ONU/ONT,其区别为 ONT 直接位于用户端，而 ONU 与用户之间还有其他网络，如以太网）以及网元管理系统（EMS)组成，通常采用点到多点的树型拓扑结构。在下行方向，IP 数据、语音、视频等多种业务由位于中心局的 OLT，采用广播方式，通过 ODN 中的 1:N 无源光分配器分配到 PON 上的所有 ONU 单元。在上行方向，来自各个 ONU 的多种业务信息互不干扰地通过 ODN 中的 1:N 无源光合路器耦合到同一根光纤，最终送到位于局端 OLT 接收端。

【问题 2】

已知网络部门对学生公寓网络分配了一个地址段 59.74.116.0/24。请给出学生公寓网络地址规划与设计方案。

【参考答案】

1. 需要配置一台 DHCP 服务器，实现内网地址的动态分配；
2. 已分配的网段不能满足用户地址分配的需求，需要相应的网络设备启用 NAT 来实现内外网地址的转换；
3. 由于属于一种类型的用户，公寓网络地址分配按选定网段顺次分配即可；
4. 需要对公寓网络进行 VLAN 和子网划分，便于降低冲突域和网络管理；
5. 为了实现子网间的频繁通信，汇聚各子网的设备具有三层交换功能。

【试题分析】

网络地址转换（NAT，Network Address Translation)属接入广域网（WAN)技术，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 不仅可以解决了 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。

虚拟局域网（Virtual Local Area Network 或简写 VLAN, V-LAN)是一种建构于局域网交换技术（LAN Switch)的网络管理的技术，网管人员可以借此通过控制交换机有效分派出入局域网的分组到正确的出入端口，达到对不同实体局域网中的设备进行逻辑分群（Grouping)管理，并降低局域网内大量数据流通时，因无用分组过多导致拥塞的问题，以及提升局域网的信息安全保障。

【问题 3】

请依据图 1-1 设计方案，并且结合用户上网方式是拨号上网、网络安全控制以及采用带内管理方式管理网络等技术因素。说明 BRAS(Broadband Remote Access Server)和 OLT 设备性能及配置描述。

【参考答案】

公寓网络的宽带认证通过 BRAS 实现，从图 1-1 网络拓扑分析，选用集成 PPPoE、DHCP、NAT、防火墙的高性能 BRAS，该 BRAS 上进行 PPPoE 的配置，为每个用户设置账号和密码：启用 DHCP 服务，配置内网地址池：进行 NAT 配置，实现内外网地址转换；进行防火墙规则配置。

OLT 可以选用具有三层交换功能的机架式、大容量、全光接入的产品，单框用户数 128 口，可以满足公寓网络的需求。对于网络系统的管理采用带内方式管理，即网管信息与业务信息共用同一通道，网管单独用 1 个 VLAN,设为 VLAN100,每个业务端口均要透传 VLAN100。

【问题 4】

如果将图 1-1 中 BRAS 设备用路由器（Router）替换，请分析在学生公寓网络规划上可能有哪些变化。

【参考答案】

1. 网络边界出现变化，学生公寓网络可作为校园网的一个子网成为校园网的一个组成部分。
2. IP 地址分配、用户认证与校园网统一，NAT、认证等功能由上端设备承担。
3. 学生公寓的网络可以有多种上联方式，可以连接校园网、Internet、IPTV、NGN 等。
4. 由于全业务路由器（Service Router)的出现，在网络规划中，路由器与 BRAS 设备在特定场合也可以实现相同的功能。

【问题 5】

请简要说明 GPON 接入相比 EPON 接入对支持“三网合一”的发展有什么优势。

【参考答案】

GPON 接入相比 EPON 接入对支持“三网合一”上的优势：

1. 速率：GPON 支持多种速率等级，可支持上下行不对称速率。EPON 提供的是固定 1.5Gbps 上下行速率。

2. 分路比：GPON 可支持 ClassA、B 和 C，可支持高达 128 的分路比和长达 20km 的传输距离。EPON 通常支持 1 ： 32 的分路比，10km 的传输距离。

3. 封装：GPON 无论是在传输汇聚层还是在业务适配层的效率都是最高的，其总效率最高，且等效系统成本最低。

【试题分析】

GPON 和 EPON 是两种主流的两种 PON 技术，GPON 符合 ITUT 的标准，而 EPON 是 IEEE 指定的标准。从速率上看 GPON 是非对成的下行 2.488G 上行 1.244G，而 EPON 上下行对称 1.25G。从分光比来看，GPON 支持最大 1:128 的分路比，而 EPON 支持 1:32; 从承载业务上看 GPON 可以承载 ATM、ETH、TDM 等多种业务而 EPON 仅支持 ETH; 在带宽效率、QoS、协议等多个方面，GPON 更具有广泛性。

试题二（共 25 分）

阅读以下关于某电信运营商网络的叙述，回答问题 1 至问题 4。

对电信运营商而言，三网融合在接入控制层面需要考虑怎样引入 IPTV，如何在多业务接入模式下实现综合运营并保障各业务的服务质量。IPoE 方式提供多业务接入以满足三网融合发展的必要性和可行性，为运营商三网融合业务提供保障。

某电信运营商 IP 城域网拓扑结构图如图 2-1 所示。

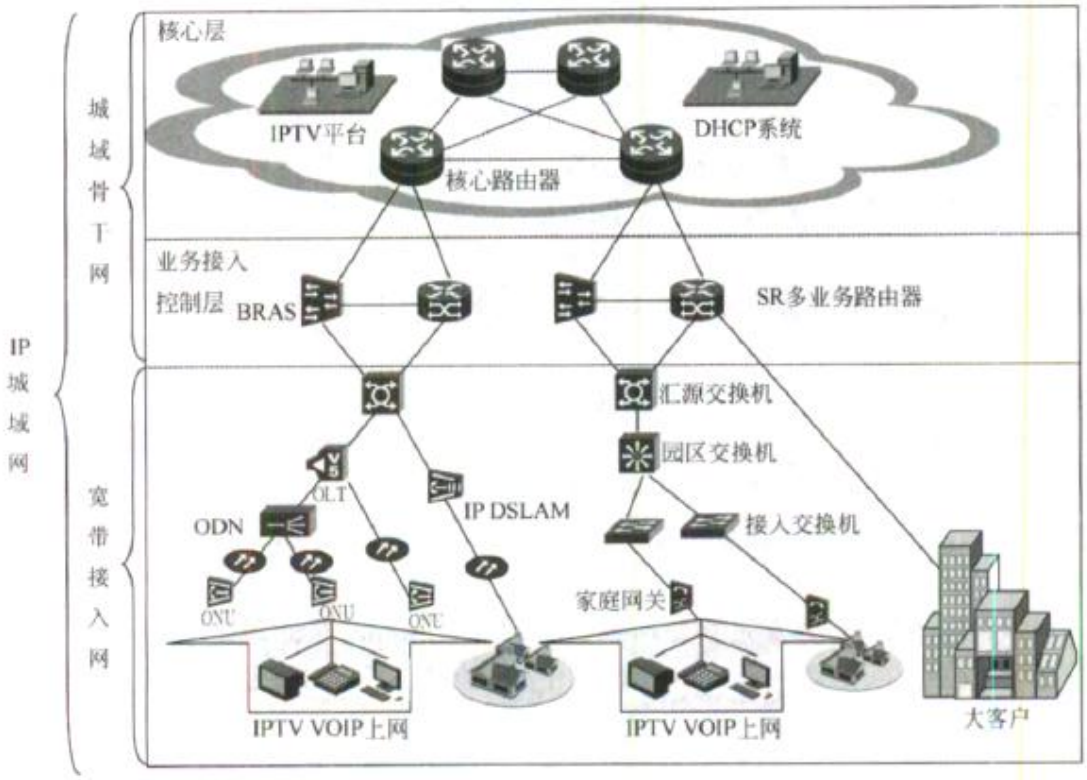


图 2-1

【问题 1】

电信运营商的网络是一种可管理网络，目前在用户管理方面得以较多的主流认证技术主要有 PPPoE、基于 Web-Portal 以及 IEEE802.1x。这三种接入认证技术由于产生的时间、背景各不相同，因此应用的网络环境也不同，各有利弊。表 2-1 是这三种认证技术的部分性能比较，请补充完成其中的空（1）~（10）。

表 2-1 三种认证技术的部分性能指标比较表

基本指标	PPPoE	Web-Portal	802.1X
组网成本	高	高	低
数据报封装开销	（1）	（2）	低
协议运行位置	（3）	（4）	数据链路层
IP 地址分配	认证后分配	（5）	（6）
接入控制	用户	用户	端口
客户端安装	需要	不需要	需要
用户连接性	好	差	好
安全性	高	低	高
业务流与控制流	不分离	（7）	（8）
支持多播业务	（9）	（10）	支持
计费统计精细度	高	低	高

【参考答案】

（1）高

（2）低

（3）数据链路层

（4）应用层

（5）认证前分配

（6）认证后分配

（7）不分离

（8）分离

（9）不支持

（10）支持

【试题分析】

本题主要考查电信运营商网络中 IPTV 的应用。

本问题主要考查运营商网络中的接入认证技术。

由于宽带业务的多样化发展趋势，用户接入认证方式作为可运营、可管理的核心， 受到包括运营商、制造商、系统集成商的密切关注。当前，电信运营商发展宽带业务主要采用的是 PPPoE 接入方式。随着 IPTV 业务的规模化发展必然进行宽带网鉟播复制点的下移，接入认证方式将发生重大变革。目前成熟的核心认证技术主要包括 PPPoE 认证、基于

Web-Portal 的认证以及 IEEE 802.1x 认证技术。

PPPoE 继承了 PPP 协议的特点，操作简单且用户较容易接受，能够很好地实现用户计费、在线检测和速率控制等功能。但是，PPPoE 的缺点也同样很明显。PPPoE 所包含的 PPP 包需要被再次封装进以太网报文内才能进行传输，封装效率受到一定影响。由于发现阶段的机制所限，会产生大量的广播包，不但使得网络承受了较大的压力，同时也使得基于组播的业务（如视频会议等）无法开展。除此之外，还需要宽带远程接入服务器 BRAS (Broadband Remote Access Server)的支持，使用这种电信级别的设备成本比较高昂，并且用户的业务数据流和控制认证流都需通过该设备，因此很容易形成网络瓶颈，降低网络性能。

基于 Web-Portal 技术的认证是一种业务类型的认证，由于使用了 Web 页面进行用户名和密码的登入验证，所以省去了安装客户端的麻烦，也避免了系统兼容性的问题。 并且，由于承载在应用层之上，无需特别的数据包封装，提高了效率，也减小了网络维护的成本。不过，也正是由于基于 Web-Portal 的认证协议处在 OSI 模型的最高层，所以对设备的要求比较高，建网的成本高。且易用性不高，标准不能统一。IP 地址在用户授权之前就已经分配给用户，不是十分合理。Web 服务器对授权用户和非授权用户来说都是可达的，因此很容易受到恶意攻击，存在安全隐患。同 PPPoE一样，用户的业务数据流和控制认证流无法区分，造成设备不必要的压力。

IEEE802.1X 就是 IEEE 为了解决基于端口的接入控制而定义的一个标准。作为基于 C/S 的访问控制和认证协议，未经授权的用户或是设备若是未通过 IEEE 802.1x 协议的认证是无法通过接入端口（Access Port)访问网络的。IEEE 802.1x 协议为二层协议不需要到达三层，业务报文直接承载在正常的二层报文上。用户通过认证后实现业务流和认证流分离，不再将数据包进行拆解。IEEE 802.1x 封装效率极高。采用了各端口独立控制处理的方式，因此认证处理容量可以很大，远远高于传统的 BRAS 设备，所有的业务流量和认证系统分开，有效的解决了网络瓶颈问题。与基于七层协议的 Web-Portal 认证相比，能够及时处理异常离线情况和实现基于时间的计费。数据分离的特点使得 IEEE 802.1x 的认证过程变得简单。整个用户认证在二层网络上实现，可以结合 MAC、端口、账户 和密码等，具有很高的安全性。由上述分析可知，这三种接入认证技术应用的网络环境不同，各有利弊。目前三种认证方式都获得了很多成功的应用：PPPoE 现在域主要的用户人群是 ADSL 用户，由电信级别的运营商提供接入服务。而基于 Web-Portal 的认证一般用于旅馆酒店，并多用于无线网络的认证。而 IEEE 802.1x 认证则普遍用于规模较大，接入用户数 R 庞大的以太网。下表就一些基本的网络数据指标对它们进行了比较。

表 三种认证技术的部分性能指标比较表

基本指标	PPPoE	Web-Portal	802.1x
组网成本	高	高	低
数据报封装开销	高	低	低
协议运行位置	数据链路层	应用层	数据链路层
IP 地址分配	认证后分配	认证前分配	认证后分配
接入控制	用户	用户	端口
客户端安装	需要	不需要	需要
用户连接性	好	差	好
安全性	高	低	高
业务流与控制流	不分离	不分离	分离
支持多播业务	不支持	支持	支持
计费统计精细度	高	低	高

【问题 2】

IPoE 和 PPPoE 都是技术较成熟的认证技术，在标准化程度、安全性、精确计费、宽带/端口的控制方面都有相似的特点。

(1) 随着 Triple Play “三重播放”业务和以广播 IPTV 为代表的多媒体业务的发展，请简单叙述采用 PPPoE 接入方式会带来的问题。

(2)目前，业界正逐步推动 PPPoE 认证技术向 IPoE 认证技术转换。请简单描述 IPoE 的特点以及大规模商用需解决的关键问题。

【参考答案】

(1)

①严重浪费 BRAS 下联链路的带宽。

②BRAS 设备的负载将非常大。

采用 PPPoE 技术承载 IPTV 类业务，造成 BRAS 设备处理能力、BRAS 与接入设备之间的带宽两个瓶颈，效率低，扩展性差，基本不能发挥组播技术的优势。

(2)

IPoE 技术的特点：支持用户会话保护，满足运营商对个人宽带业务认证、计费需求；高效的组播传播，适合 IPTV 业务；长接在线，适合语音及视频电话业务；减少多余开销，提高传输效率。

IPoE 技术需要解决的问题：IPoE 认证没有像 PPPoE 认证那样在网络层面提供唯一的点到点的通信机制，运营商在部署 IPoE 认证时，要重点关注安全问题。如：DHCP 溢出攻击、

ARP 溢出攻击、Session 终结管理等。

【试题分析】

本问题主要考查在电信运营商的 IPTV 实施中 IPoE 和 PPPoE 各自的技术特点。

(1) 对于大量的视频流，只有通过组播方式传送才能最大化地利用带宽，缓解网络瓶颈。而 PPPoE 数据包，给所有数据包都封装 PPP 包头，在 BRAS 与所连接的上万个宽带用户终端之间建立了相同数最的点对点连接。这种方式决定了 BRAS 到所有终端都是唯一的点到点链路，二者之间的任何二层设备对所传送的数据包都没有办法进行组播复制。因此，采用 PPPoE 封装传送广播 IPTV 组播数据流，BRAS 设备会在所有到用户终端的点到点连接上复制组播数据流。这就造成大量数据包在 BRAS 以下的交换机和 EPON 单元上被束复传送，严重浪费 BRAS 下联链路的有限带宽。

BRAS 设备要时刻接受用户拨入请求，与 Radius 服务器合作完成用户的认证工作，同时还要维护大量的 PPPoE 状态信息，对设备的要求是比较高的。IPTV 数据流量大，要求低时延，线速转发，如果进行 PPPoE 数据包封装，在用户量稍大时，BRAS 设备的负载将非常大。采用 PPPoE 技术承载 IPTV 类业务，造成 BRAS 设备处理能力、BRAS 与接入设备之间的带宽两个瓶颈，效率低，扩展性差，基本不能发挥组播技术的优势。

(2) IPoE 认证方式不需要在用户终端上安装任何客户端程序，不需要输入用户名和密码，非常适合新型网络设备，如智能手机，数字电视，PSP (PlayStationPortable,多功能掌机系列，具有游戏、音乐、视频等多项功能）等很难支持内置的 PPPoE 拨号程序的终端应用互联网业务。IPoE 技术的特点：支持用户会话保护，满足运营商对个人宽带业务认证、计费需求；高效的组播传播，适合 IPTV 业务；长接在线，适合语音及视频电话业务；减少多余开销，提高传输效率。

IPoE 技术需要解决的问题：IPoE 认证没有像 PPPoE 认证那样在网络层面提供惟一的点到点的通信机制，运营商在部署 IPoE 认证时，要重点关注安全问题。如：DHCP 溢出攻击和应对策略：ARP 溢出攻击和应对策略：Session 终结管理，根据 DHCP 协议的特性，当 Session 终结后，用户的 IP 地址并不能及时释放并回收。

【问题 3】

IPoE 部署需要从运营支撑系统、核心层、业务控制层和接入层分别进行部署。

（1）图 2-1 的 IPoE 部署采用的是多边缘架构进行业务接入区分优化，请对其进行简要

描述。

（2）如果对 IPoE 部署采用单边缘架构的部署方案，请对图 2-1 简单修改并画出其拓扑结构。

（3）比较多边缘和单边缘两种 IPoE 部署方案的优缺点。

【参考答案】

(1)

①核心层的设备保持不变，在业务接入控制层根据不同的业务需求进行设备接入区分优化。将宽带接入服务器（BRAS)作为使用 PPPoE 上网业务的边缘控制设备，业务路由器（SR)作为使用 IPoE 的 IPTV、流媒体等关键业务的边缘控制设备，形成多边缘的网络架构。

②宽带接入网主要将接入层设备改造成支持 IPoE 和多播的设备。接入层设备包括 OLT、EPON、园区交换机和楼道交换机等。

(2)

①城域骨干网核心层的设备保持不变，在业务接入控制层选择新建全业务路由器，或升级现网 BRAS 为全业务网关来负责业务统一接入，具备 BRAS 和 SR 的功能，形成单边缘的网络架构；

②宽带接入网主要将接入层设备改造成支持 IPoE 的设备。接入层设备包括 OLT、EPON、园区交换机和楼道交换机等。

(3)

多边缘的网络架构：

优点：现网结构保持不变或改动小，投资较小；上网业务和视频等业务区分接入，可满足不同业务的需求。

缺点：多边缘的网络架构存在多张计费清单，存在同步等问题；对接入层设备要求高，需对不同业务做分离，接入层 QoS 策略复杂。

单边缘的网络架构：

优点：全业务统一接入，便于业务管理；简化了业务控制层的结构及设备维护；简化接入层 QoS 的策略部署。

缺点：现网结构改动大，投资大。

【问题 4】

目前电信运营商的用户采用 IPoE 的宽带接入主要认证场景为大客户专线接入认证、IPTV 等，IPoE 和 PPPoE 的交叉场景就是 IPTV，下面就 IPTV 应用 IPoE 和 PPPoE 的场景进行分析。

（1）请在图 2-2 中分别完成 IPTV 使用 PPPoE 和 IPoE 认证方式时多播放视频流的流向和流数，并予以简单说明（其中，采用 IPoE 时多播复制点选择在园区交换机和 OLT 上）。

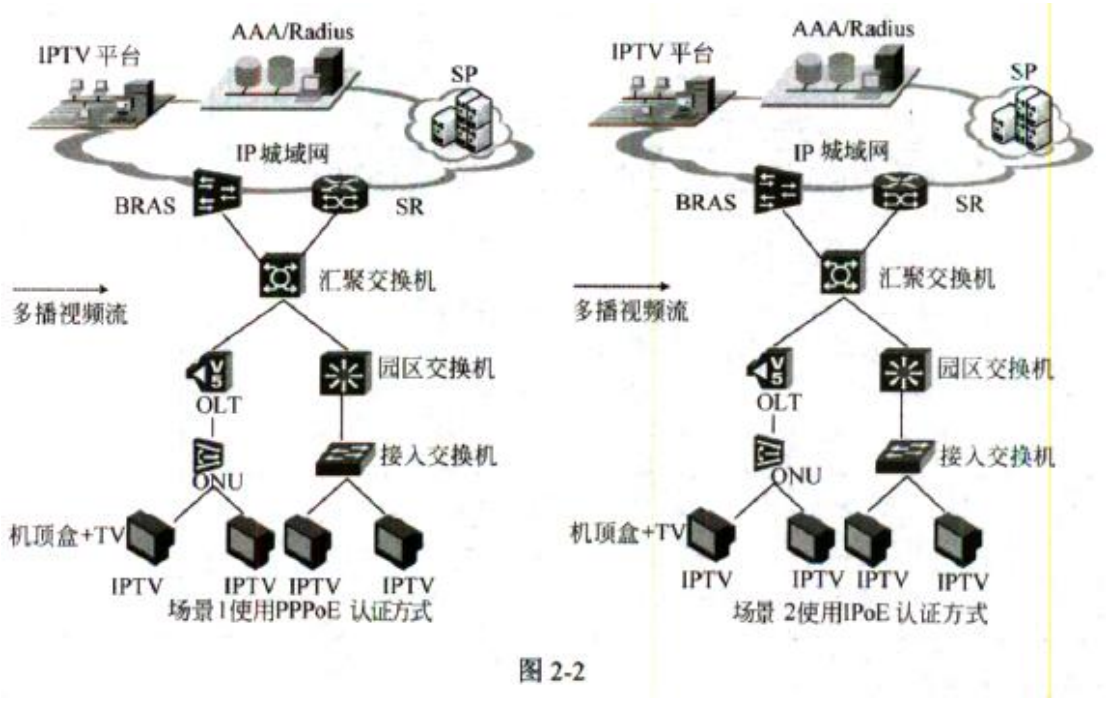


图 2-2

（2）请根据上述比较简要叙述 IPTV 业务发展不同阶段时的认证方式选择。

【参考答案】

(1)

场景1使用PPPoE认证方式

场景2使用IPoE认证方式

①使用 PPPoE 认证，IPTV 的多播复制点只能是 BRAS。

如场景 1 所示，多播复制点为 BRAS，BRAS 面向每个 IPTV 用户都要复制一份数据。这种场景对 BRAS 下行链路（BRAS—汇聚交换机）的带宽，园区交换机、OLT 的上行链路（园区交换机、OLT—汇聚交换机）的带宽及 IP 城域网带宽资源造成很大的压力。

②使用 IPoE 认证，IPTV 的多播复制点可以灵活选择在 OLT、IP DSLAM、汇聚交换机、园区交换机、接入交换机。

如场景 2 所示，多播复制点为园区交换机和 OLT，由园区交换机、OLT 面向每个 IPTV 用户进行数据复制。大大节省了带宽资源，降低 BRAS 压力。

(2)根据上述比较，在 IPTV 发展初期，用户规模比较小时，运营商往往采用 BRAS 接入，通过 PPPoE 协议认证。随着用户规模的逐步扩大，PPPoE 的缺点逐渐显露，加之建设成本高。因此，在 IPTV 业务快速发展时，运营商宜采用 IPoE 方式承载 IPTV。

【试题分析】

本问题主要考查 IPTV 的实际应用场景。

目前电信运营商的用户采用 IPoE 的宽带接入主要认证场景为大客户专线接入认证、IPTV 等。IPoE 和 PPPoE 的交叉场景就是 IPTV，下面就 IPTV 应用 PPPoE 和 IPoE 的不同场景进行分析。

场景 1:使用 PPPoE 认证方式

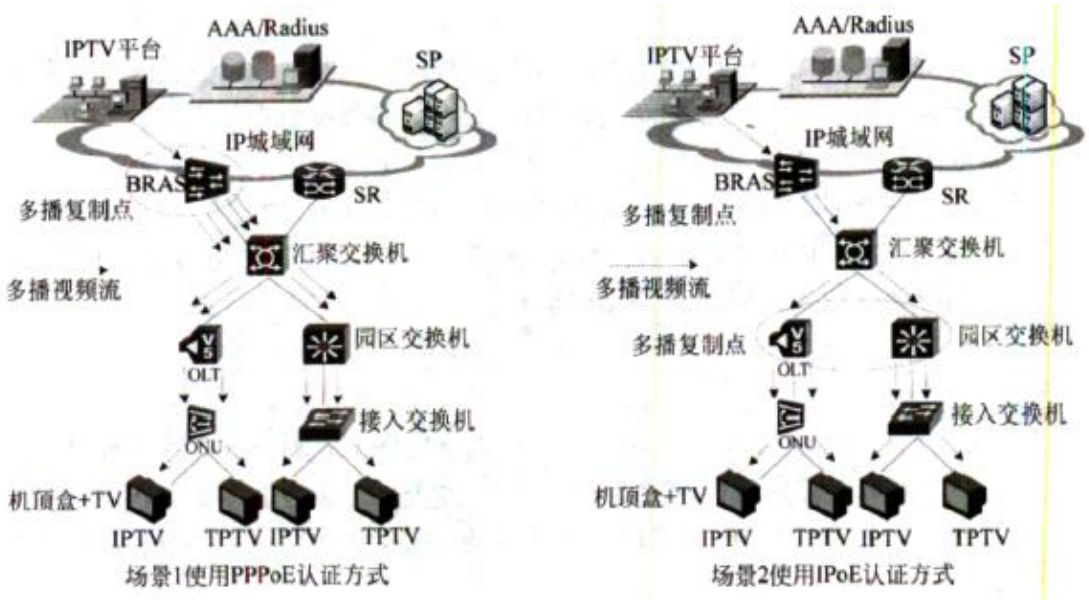
使用 PPPoE 认证，IPTV 的多播复制点只能是 BRAS。如图 2-2 所示，多播复制点为 BRAS，BRAS 面向每个 IPTV 用户都要复制一份数据。这种场景对 BRAS 下行链路（BRAS—汇聚交换

机）的带宽，园区交换机、OLT 的上行链路（园区交换机、OLT—汇聚交换机）的带宽及 IP 城域网带宽资源都造成了很大的压力。

场景 2:使用 IPoE 认证方式

使用 IPoE 认证，IPTV 的多播复制点可以灵活选择在 OLT、IPDSLAM、汇聚交换机、园区交换机、接入交换机。如图 2-2 所示，多播复制点为园区交换机和 OLT，由园区交换机、OLT 面向每个 IPTV 用户进行数据复制。这种场景大大节省了 BRAS——园区交换机、OLT 链路的带宽资源，降低了 BRAS 压力。采用 IPoE,播复制点可选择最靠近用户的设备上，也可采用多级复制、逐级复制进行组播流最的优化。

下图是 IPTV 使用 PPPoE 和 IPoE 认证方式时多播视频流的流向和流数(其中,采 用 IPoE 时多播复制点选择在园区交换机和 OLT 上）



根据上述比较，在 IPTV 发展初期，用户规模比较小时，运营商往往采用 BRAS 接入，通过 PPPoE 协议认证。随着用户规模的逐步扩大，PPPoE 的缺点逐渐显现出来，联带建设成本高，因此，在 IPTV 业务快速发展时，运营商更倾向于采用 IPoE 方式承载 IPTV。

试题三（共 25 分）

阅读下列说明，回答问题 1 至问题 5,将解答填入答题纸的对应栏内。

【说明】

图 3-1 是某制造企业网络拓扑、该企业包括制造生产、研发设计、管理及财务、服务器群和销售部等五个部分。该企业通过对路由器的配置、划分 VLAN、使用 NAT 技术以及配置 QoS 与 ACL 等实现对企业网络的安全防护与管理。

随着信息技术与企业信息化应用的深入融合，一方面提升了企业的管理效率，同时企业在经营中面临的网络安全风险也在不断增加。为了防范网络攻击、保护企业重要信息数据，企业重新制定了网络安全规划，提出了改善现有网络环境的几项要求。

1. 优化网络拓扑，改善网络影响企业安全运行的薄弱环节；
2. 分析企业网络，防范来自外部攻击，制定相应的安全措施；
3. 重视企业内容控制管理，制定技术方案，降低企业重要数据信息的泄露风险；
4. 在保证 IT 投资合理的范围，解决远程用户安全访问企业网络的问题；
5. 制定和落实对服务器群安全管理的企业内部标准。

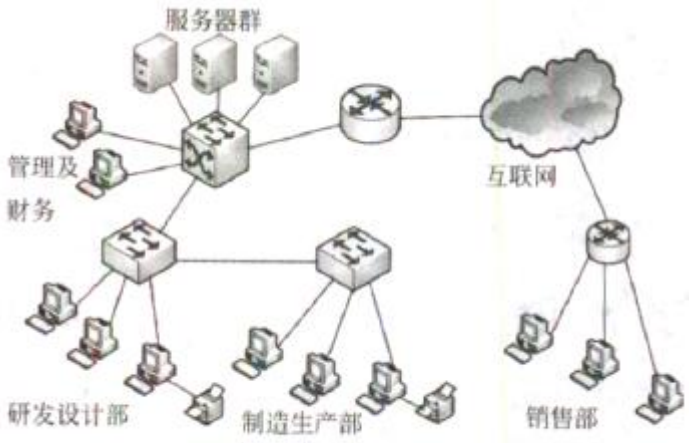


图 3-1

【问题 1】

请分析说明该企业现有的网络安全措施是如何规划与部署的，应该从哪个角度实现对网络的安全管理。

【参考答案】

1. 接入交换机上进行访问控制；
2. VLAN 技术通过用户隔离，实现对敏感信息的访问进行限制；

3. 在边界路由器上配置 NAT，屏蔽内网地址信息，降低外部的攻击；

4. 边界路由器上配置 ACL 访问控制列表，可以实现策略控制，进行访问权限控制。

【试题分析】

本题考查局域网络安全的相关知识，包括 NAT、VLAN, GAP(网闸)、ACL、VPN 等的综合运用以及网络安全拓扑的规划、管理等内容。

该企业现有的网络需要进行多级的安全部署。首先在接入层交换机上进行访问控制；采用 VLAN 技术通过用户隔离，实现对敏感信息的访问进行限制：在边界路由器上配置 NAT，屏蔽内网地址信息，降低外部的攻击：边界路由器上配置 ACL 访问控制列表，可以实现策略控制，进行访问权限控制。

【问题 2】

请分析说明该企业的网络拓扑是否存在安全隐患，原有网络设备是否可以有效防御外来攻击。

【参考答案】

1. 制造生产部子网络应该直接接入核心交换机，该网络中当研发部子网络的交换设备故障时将会直接对制造生产部的一线产生影响；

2. 在内部网和外部网之间、专用网与公共网之间没有专门的防护设备，不能防御外来攻击；

3. 服务器群应设置在防火墙的 DMZ 区；

4. 应当配备 IPS 设备、流量监控、上网行为管理和网络病毒防护设备：

5. 采用网闸物理隔离财务部门和有关涉密部门。

【试题分析】

该企业现有的网络存在诸多安全隐患：

GAP 全称安全隔离网闸。安全隔离网闸是一种由带有多种控制功能专用硬件在电路上切断网络之间的链路层连接，并能够在网络间进行安全适度的应用数据交换的网络安全设备。

【问题 3】

入侵检测系统（IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。请简要说明该企业部署 IDS 的必要性以及如何在该企业网络中部署 IDS.

【参考答案】

必要性：

1.防止内部人员攻击；

2. 和防火墙互为补充；

3. 攻击发生后的取证。

部署：采用旁路方式接入核心交换机

【试题分析】

入侵检测系统（IDS)是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。通常 IDS 采用旁路方式接入核心交换机，可以和防火墙互为补充，防止内部人员攻击，攻击发生后的取证等。

【问题 4】

销售部用户接入企业网采用 VPN 的方式，数据通过安全的加密隧道在公共网络中传播，具有节省成本、安全性高、可以实现全面控制和管理等特点。简要说明 VPN 采用了哪些安全技术以及主要的 VPN 隧道协议有哪些。

【参考答案】

VPN 采用的安全隧道技术包括：加解密技术、密钥管理技术、身份认证技术。

VPN 协议有：PPTP、L2PT、IPSec。

【试题分析】

VPN（虚拟专用网络）是指在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。VPN 有多种分类方式，主要是按协议进行分类。VPN 可通过服务器、硬件、软件 等多种方式实现，VPN 具有成本低，易于使用的特点。主要采用的协议有：在互联网上建立 IP 虚拟专用网隧

道的协议 PPTP;建立在点对点协议 PPP 的基础上，把各种网络协议（IP、IPX 等）封装到 PPP 帧中，再把整个数据帧装入隧道协议 L2TP;对 IP 协议分组进行加密和认证的协议 IPSec。

【问题 5】

请结合自己做过的案例，说明在进行企业内部服务器群的安全规划时需要考虑哪些因素。

【参考答案】

1. 首先划分信息安全级别

2. 依据安全级别，考虑以下内容：

(1) DMZ 区安全防护

(2) 机房的物理安全

(3) 主机的系统安全

(4) 数据备份机制

(5) 安全管理制度

【试题分析】

任何企业在做安全规划时，首先依据需求划分信息安全级别，然后依据安全级别，考虑 DMZ 区安全防护，机房的物理安全，主机的系统安全，数据备份机制，安全管理制度等等。

试题一 论网络中心机房的规划与设计

随着计算机的发展和网络的广泛应用，越来越多的单位建立了自己的网络，网络中心机房的建设是其中一个重要环节。它不仅集建筑、电气、安装、网络等多个专业技术于一体，更需要丰富的工程实施和管理经验。网络中心机房设计与施工的优劣直接关系到机房内计算机系统是否能稳定可靠地运行，是否能保证各类信息通信的畅通。

请以“网络中心机房的规划与设计”为题，依次对一下三个方面进行论述。

1. 概要叙述你参加设计的网络项目以及你所担任的主要工作。

2. 具体讨论在网络中心机房的规划与设计中的主要工作内容和你所采用的原则、方法和策略，以及遇到的问题和解决措施。

3. 分析你所规划和设计网络中心机房的实际运行效果。你现在认为应该做哪些方面的改进以及如何加以改进。

【写作要点】

1. 机房工程整体建设。
2. 防静电地板铺设。
3. 隔断装修。
4. UPS 不间断电源。
5. 精密空调系统。
6. 新风换气系统。
7. 接地系统。
8. 防雷系统。
9. 监控系统。
10. 门禁系统。
11. 漏水检测系统。
12. 机房环境及动力设备监控系统。
13. 消防系统。
14. 屏蔽系统。

试题二 大型企业集团公司网络设计解决方案

公司为了发展业务、提高核心竞争能力，希望新建一个快捷安全的通信网络综合信息系统。该公司网络的基本需求如下：

1. 公司办公地点分布在多个地方。在A城市除了公司本部外还有一个相距10公里的生产工厂，在相距1000公里外的B城市有一个研发部门，还有遍布全国30个大中城市的营销公司也需要联网。

2. 网络用户除固定的桌面系统外还有移动终端上网需求。

3. 公司本部包括经理办公室、生产部、市场部、人力资源部等多个办公部门，共有信息点3000个（不包括移动终端，下同），生产共产和研发部也划分为一些科室，各有信息点1000个左右。

4. 建立一个符合开放性规范的综合业务通信网络，集成OA办公和企业管理，能够进行数据、声音、图像综合传输的网络平台。

5. 网络要符合下列要求：先进性、通用性和容错性，可扩展可审计，便于维护管理，性价比高。

请以“大型企业集团公司网络设计解决方案”为题，依次对一下四个方面进行论述。

1. 根据你自己参与的网络规划和建设项目，参考常见的网络设计方案，按照以上要求给出本网络的解决方案。

2. 描述网络连接拓扑结构、设备选型和地址分配等具体方案。

3. 概述网络安全解决方案，分析方案的优缺点及选择依据。

4. 在实际网络设计项目中需重点解决的问题。

【写作要点】

一、网络拓扑结构闯

二、设备选型

1.核心层交换机的选择

核心骨干设备的选择最为重要，要根据业务需求和未来发展规划，在5个重要的性能指标方面进行选择。

(1) 网络接口类型：必须具有10M/100M/1000M端口。10G以太网可以作为可选项，根

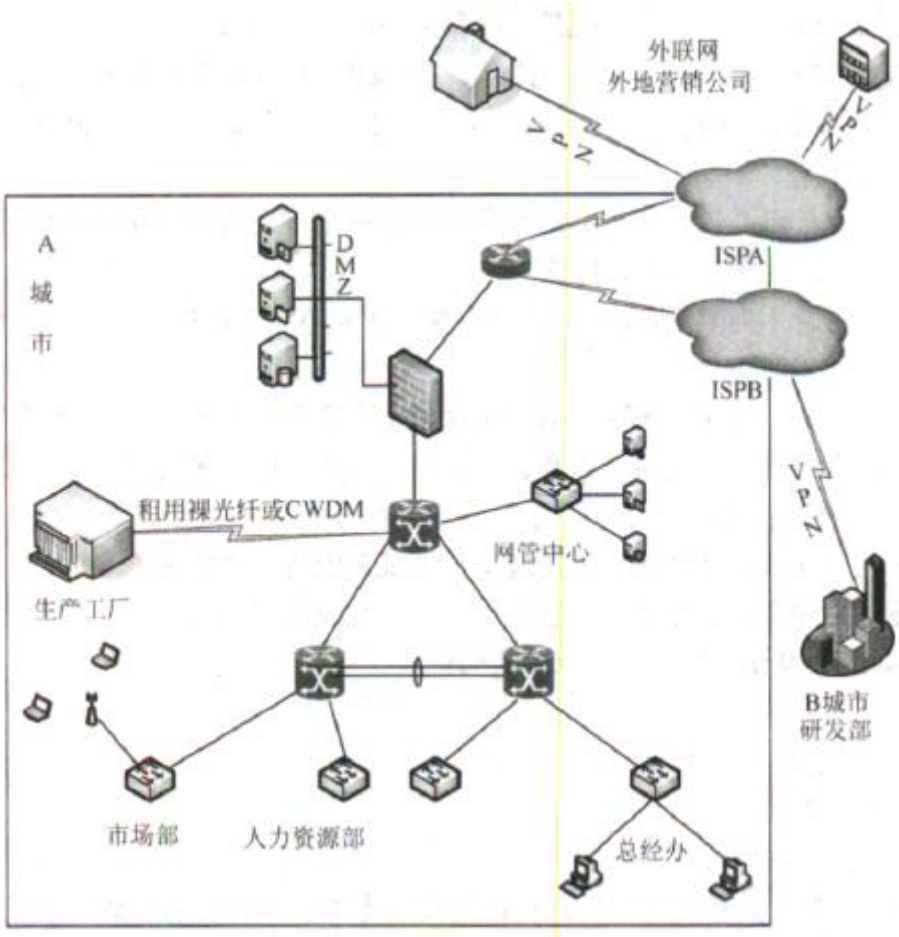
据网络业务和未来发展规划确定是否必备。骨干以太网交换机大都支持广域网端口，并提供城域间网络连接，CWDM 支持也是设备选型时的重要参考。

(2) 吞吐量指标：吞吐量反映了交换机对数据包的拆分、封装、策略处理、转发/ 路由数据包的能力。核心交换设备的最高性能是无阻塞地实现数据交换，不仅应该提供二层以太帧的线速转发，而且应该提供三层数据包的线速转发。

(3) 可用性指标：交换机是否支持关键模块（电源、风扇、交换矩阵、CPU 等）的冗余；链路层是否具备弹性恢复功能，网络层是否支持动态路由协议，是否支持等价多路由功能，是否支持网关冗余协议(VRRP)。

(4) 单/组播协议：必须支持单播路由协议和多路广播路由协议。作为骨干交换机必须支持 RIPv1、RIPv2、OSPF 等路由协议，这些路由协议能够很好地互通，其他路由协议根据具体的需求来确定是否必需。

(5) QoS 保障：这是在网络拥塞时确保高优先级流童获得带宽的技术。由于关键的多媒体应用大量涌现，要求交换机硬件支持优先级队列的数量越来越多，仅支持 2～3 个硬件优先级队列的产品已不能满足用户的业务需求。



当前市场上核心交换机比较常用的有锐捷网络系列核心路由交换机、 Cisco Catalyst 6500 系列，D-Link DES-7600、D-Link DES-6500 等。

2.汇聚层交换机的选型

汇聚层交换机必须具有交换路由、可管理、高 QoS 保障、高安全性，以及支持多业务应用特性等功能。

可对网络及设备监控和管理。用户在选择交换机产品时，除了能满足对整个网络节点的拓扑发现、流量监控、状态监控等需求以外，还应对交换机提出远程配置、用户管理、访问控制乃至 QoS 监控等要求。

提供 QoS 保障功能。必须具有对不同应用类型数据进行分类处理（QoS)的功能，实现端到端的 QoS 保障，因而这要求交换机支持 802.1p 优先级、IntServ (RSVP)和 DiffServ 等功能。

要求汇聚交换机支持多媒体应用。整个网络的发展趋势是朝着网络融合以及应用融合的趋势发展，对于支持语音、组播等功能的交换机产品应优先考虑。

进行访问控制。网络变得越来越智能化，而在汇聚层设备上实现用户分类、权限设认证、计费）、802.1x 等多种安全认证方式。

高安全性。为确保核心交换机不受类似拒绝服务（DoS)等攻击而导致全网瘫痪，不但要在核心交换机中采用防火墙和 IDS 预防和检测攻击的技术，在汇聚层交换设备中也必须增加此项功能，更好地实现全网安全。

比较常见的汇聚层交换机有华为 Quidway S5000 系列、Quidway S5600 系列等，锐捷 RG-5700 系列、RG-S4009 系列等，Cisco Catalyst 4500 系列、Cisco Catalyst 3700 系列等。

中低端交换机的生产厂商很多，主要有 Cisco (思科)、Juniper (杰科)、H3C (华为 3COM)、中兴通信等公司。

3. 防火墙产品的选择

防火墙是在内部网和外部网之间、专用网与公共网之间构造的保护屏障，它是计算机硬件和软件的结合，从而保护内部网免受非法用户的入侵。防火墙主要由服务访问策略、验证工具、包过滤和应用网关 4 个部分组成。

以防火墙所采用的技术不同来区分，可分为：①包过滤型；②代理型；③监测型。新一代监测型防火墙能够对各层数据包进行主动的、实时的监测，有效地判断各层中的非法侵入。同时，检测型防火墙一般还带有分布式探测器，这些探测器部署在各种应用服务器和

各个网络节点之中，不仅能够检测来自网络外部的攻击，同时对来自内部的恶意破坏也有极强的防范作用。例如 CISCO ASA5505-UL-BUN-K8。

4. 路由器的选型

根据下列指标进行选择：

(1) 路由协议

路由器是用来连接不同网络的，这些不同的网络可能采用不同的路由协议。这就要求在选配路由器时注意它所支持的网络协议有哪些，特别是对于广域网中的路由器。

(2) 背板能力

通常是指路由器背板容量或总线带宽。中档路由器的包转发能力均应在 IMpps 以上。这个性能对于保证整个网络之间的连接速度是非常重要的。

(3) 丢包率

丢包率是指在一定的数据流量下，路由器不能正确进行转发的数据包在总数据包中所占的比例。正常工作的路由器丢包率应小于 1%。

(4) 转发延迟

路由器的转发延迟指从转发的数据包最后一比特进入路由器端口，到该数据包第一比特出现在出口链路上的时间间隔，通常用毫秒计算。这个参数通常在路由器端口吞吐量范围内进行测试。

(5) 路由表容量

路由表容量是指路由器运行中可以容纳的路由数量。一般来说，路由器越高档，路由表容量越大。这一参数与路由器自身所带的缓存大小有关。

(6) 可靠性

可靠性是指路由器的可用性、无故障工作时间和平均故障修复时间等指标，这一指标对新买的路由器无法验证。所以应该选择信誉较好、技术先进的品牌。

(7) 网管能力

在大型网络中，路由器支持标准的网管系统尤为重要。一般的路由器厂商都会提供一些与之配套的网络管理系统软件。选择路由器时，务必要关注网络系统的监管和配置能力是否强大，设备是否可以提供统计信息和深层故障检测的诊断功能等。

三、地址分配方案

入口路由器进行 NAT 地址变换；通过 DHCP 服务器分配内部私网地址；每个二级单位组成一个 VLAN，地址空间分配如下：

10.0.0.0/8	集团公司全部地址空间
10.16.0.0/13	集团公司本部全部地址空间
10.16.64.0/17	集团公司网管类全部地址
10.16.128.0/17	集团公司互联类全部地址
10.16.196.0/17	集团公司应用类全部地址
10.16.196.0 /21	集团公司总经办地址空间
10.16.200.0/21	集团公司生产部地址空间
10.16.204.0/21	集团公司市场部地址空间
10.16.208.0/21	集团公司后勤部地址空间
10.16.212.0/21	集团公司人力资源部地址空间
10.16.216.0/21	.....地址空间
10.16.220.0/21	.....地址空间
10.16.224.0/21	.....地址空间

四、网络安全解决方案

设置防火墙保护内部网络免受非法用户的入侵；旁路接入 IDS 和 IPS 设备，监测网络入侵以及网络病毒的危害；在汇聚交换机上安装用户上网行为管理设备和流量监测设备；采用安全有效的用户认证方案，结合 Windows 域用户管理和审计功能，严格实施网络资源的访问控制。

五、重点解决的问题

根据自己熟悉的领域，在需求分析、设备选型、网络安全解决方案等方面进行略微详细的论述。