TDM 和 FDM 是实现多路复用的基本技术，有关两种技术叙述正确的是(1)。

(1)A.TDM 和 FDM 都既可用于数字传输，也可用于模拟传输

B.TDM 只能用于模拟传输，FDM 只能用于数字传输

C.TDM 更浪费介质带宽，FDM 可更有效利用介质带宽

D.TDM 可增大通信容量，FDM 不能增大通信容量

【答案】C

【解析】本题考查时分多路复用(TDM)和频分多路复用(FDM)的基础知识。

TDM(Time-Division Multiplexing)方法的原理是把时间分成小的时隙(Time slot)，每一时隙由一路信号占用，每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙，每个用户所占用的时隙周期性地出现。显然，时分复用的所有用户在不同的时间占用全部的频带带宽。在进行通信时，复用器和分用器总是成对地使用，在复用器和分用器之间是用户共享的高速信道。如果一个用户在给定的时隙没有数据传送，该时隙就空闲，其他用户也不能使用，因为时隙的分配是事先确定的，接收方根据事先分配的时间确定在哪个时隙接收属于自己的数据。TDM 用于数字传输。

FDM(Frequency-Division Multiplexing)的基本原理是将多路信号混合后放在同一传输介质上传输。多路复用器接收来自多个数据源的模拟信号，每个信号有自己独立的频带。这些信号被组合成另一个具有更大带宽、更加复杂的信号，合成的信号被传送到目的地，由另一个多路复用器完成分解工作，把各路信号分离出来。FDM 用于模拟传输。

带宽为 3KHz 的信道，在无噪声条件下传输二进制信号的极限数据率和在信噪比为 30dB 条件下的极限数据率分别为(2)。该结果说明(3)。

(2)A.6Kbps，30Kbps　　B.30Kbps，6Kbps　　C.3Kbps，30Kbps　　D.3Kbps,3Kbps

(3)A.结果一样　　B.有噪声时结果更好

C.无噪声时结果更好　　D.条件不同不可比

【答案】A　　D

【解析】本题考查有关带宽与数据率的关系及数据率计算方法的基础知识。

其计算方法为：对没有噪声的信道，利用奈奎斯特准则计算信道的极限数据率，该准则为：在带宽为 W(Hz)的无噪声信道上传输信号，假定每个信号取 V 个离散电平值，则信道的极限数据率(比特率)为

2W*log2V(bps)

对有噪声的信道，利用香农定理计算信道的极限数据率，该定理为:在带宽为W(Hz)的有噪声信道上传输信号，假定信噪比为S/N(功率比)，则信道的极限数据率为

W*log2(1+S/N)(bps)

上述两个计算公式的条件是不一样的。对奈奎斯特准则，考虑每个信号可表示的状态数是V，其特例是V=2，即每个信号可表示两个状态之一(0或1)。而香农定理不限制每个信号表示的状态数。

传输介质越长,传播延迟越大,由此导致的延迟失真越大。受延迟失真影响最大的是(4)。

(4)A.低速、数字信号　　B.高速、数字信号

C.低速、模拟信号　　D.高速、模拟信号

【答案】B

【解析】本题考查传输损害方面的基础知识。

延迟失真是有线传输介质独有的现象,这种变形是由有线介质上信号传播速率随着频率而变化所引起的。在一个有限的信号频带中，中心频率附近的信号速度最高，而频带两边的信号速度较低，这样，信号的各种频率成分将在不同的时间到达接收器。

延迟失真对数字信号影响尤其重大，一个位元的信号成分可能溢出到其他的位元，引起信号内部的相互串扰，这将限制传输的位速率。

当千兆以太网使用UTP作为传输介质时，限制单根电缆的长度不超过(5)米，其原因是(6)。

(5)A.100　　B.925　　C.2500　　D.40000

(6)A.信号衰减严重　　B.编码方式限制

C.与百兆以太网兼容　　D.采用CSMA/CD

【答案】A　　D

【解析】本题考查以太网的基本原理。

传统以太网采用CSMA/CD访问控制方式，规定单根UTP电缆的长度不超过100m，最大介质长度以及最小帧长度的确定原则是：能确保一个帧在发送过程中若出现冲突，则一定能够发现该冲突。发展到千兆以太网，虽然数据率提高，但访问方式(帧的发送与接收方式)、帧的格式、介质长度维持不变，以保持与传统以太网的兼容。

介质的最长长度确定了时间片(信号在介质上往返传输的时间)的长度：假定节点A、B

分别在总线的两端，A 首先向 B 发送信息。假定 A 发送的信息即将到达 B 时，B 开始向 A 发送信息，此时 B 没有检测到冲突，但刚刚开始发送后 A 的信息到达，B 检测到了冲突。B 发送的信息到达 A 后，A 检测到了冲突。从这一过程，我们可以得出下述结论：

(1)为确保一个节点(如 A)在任何时候都能够检测到可能发生的冲突，需要的时间是信号在总线上往返传输的时间，此时间被称为时间片，也称为冲突域、冲突窗口、争用期，而这个时间是由介质的长度决定的。

(2)为保证在冲突发生后能够检测到冲突，必须保证在冲突发生并被检测到时，帧本身没有发送完(因为发送完后即使出现了冲突也不检测)，因此需要为帧设定一个最短长度。

(3)争用期、最短帧长度确定了，介质的最大长度也就确定了。这也是为什么局域网的介质长度都受到严格限制，而广域网的长度无此限制的原因。

对无线局域网，可显著提高数据率的技术是(7)，对有 2 台计算机、1 个 AP、采用 300Mbps 的 802.11n 的 WLAN，2 台计算机数据传输的概率相同，则每台计算机实际传送用户数据的最大理论速度最接近(8)MB/S。

(7)A.CSMA/CA　　B.CSMA/CD　　C.CDMA　　D.MIMO

(8)A.1.4　　B.6.7　　C.9.3　　D.18.7

【答案】D　D

【解析】本题无线局域网(WLAN)的基本知识。

WLAN 采用 CSMA/CA 访问控制方式，多台计算机竞争使用一个信道与 AP 通信以发送数据，计算机越多，冲突的机会越多，每台计算机实际获得的发送数据的机会越少，这种方式限制了一个 AP 可服务的计算机的数量即网络的规模。

MIMO 方式利用多个天线，分别使用不同的信道(频率)，可同时传输更多的信号，使得一台计算机与 AP 之间的数据率显著提高，也允许更多的计算机同时传输数据。

对于 2 台计算机、1 个 AP 的情况，因发送概率相同，则每台计算机获得的实际数据率可认为是总带宽的一半即 150Mbps，换算成以字节为单位的数据率 18.75MB/S。

此题可进一步精确：WLAN 帧最大长度为 2346B，其中数据部分最大长度为 2312B，所以每台计算机实际发送用户数据的最大理论速度的近似值可表示为 18.75MB/S*2312/2346≈18.5MB/s。

阻塞包算法(反馈抑制法)是一类典型的基于闭环控制原理的拥塞控制方法，其主要缺点

之一是(9)。

(9)A.显著降低通信效率　　B.可能导致不公平

C.不能真正控制拥塞　　D.降低网络可用性

【答案】B

【解析】本题考查拥塞控制方面的基本知识。

阻塞包算法是利用闭环原理实现拥塞控制的一种方案，其目标是在拥塞发生时起作用，而在没有拥塞时不起作用，以最大限度地提高系统的吞吐量和效率。

阻塞包算法假设每条输出线有两个变量μ和f，μ为近期利用率，其值为0≤μ≤1，f为瞬时利用率，其值为0或1。定义公式μ新=aμ旧+(1-a)f，α取0～1之间的数值，反映输出线利用率修改的周期。可为μ定义一个阈值，当μ大于此值时，进入报警状态，否则算法不起作用。

阻塞包算法的工作过程可描述为：

①　(测量)节点收到包，重新计算μ值。

②　②(判断)根据μ值判断是否为报警状态？

若不是，则转发包，转①处理下一个包。

若是，则转③。

③(报警)判断该包在其他节点上是否触发发送过阻塞包？

若没有，则向源节点发送一个阻塞包，同时在收到的数据包上填入已发阻塞包标志。

转发包，转①。

④(抑制)源节点在收到阻塞包后，将发送包的速度降低X%。当在规定的时间间隔τ内如果没有收到新的阻塞包，就将发送速度提高Y%(Y<X)

该算法的缺点之一是可能导致不公平。源端主机在收到阻塞包后需要降低发送速度，但是可能会因某种原因导致多个数据源收到阻塞包的时间上有差异，使得有些源端因发送速度快已发送完而没有降低发送速度，有些源端因发送速度慢或数据多没有发送完而降低了发送速度，从而可能造成一种“慢的更慢”的情况，这对各主机来说是不公平的。

距离向量路由算法要求每个节点保存一张距离向量表(即路由表)，其中最关键的路由信息是(10)。

(10)A.源节点到目的节点的最短距离

B.源节点到目的节点的路径

C.本节点到目的节点的输出节点(下一节点)地址

D.本节点到目的节点的路径

【答案】C

【解析】本题考查路由算法与协议方面的基本知识。

距离向量路由算法要求每个节点保存一张距离向量表(即路由表),其中包括各目的节点、本节点到对应目的节点的最短距离、本节点到目的节点的输出节点(下一节点)地址。

SDH 网络是一种重要的广域网，具有多种网络结构，可简述为(11)。

(11)A.星型网结构借助 ATM 设备连接，主要用作专网

B.链型网结构借助 DXC 设备连接，主要用作接入网

C.环型网结构借助 ADM 设备连接，主要用作骨干网

D.网孔型结构借助 ADM 设备连接，主要用作长途骨干网

【答案】C

【解析】本题考查 SDH 网络的基本知识。

SDH 网络是一种重要的广域网，具有多种网络结构，主要有：利用 ADM 连接的链型网、利用 DXC/ADM 连接的星型网、利用 DXC/ADM 连接的树型网、利用 ADM 连接的环型网、利用 DXC/ADM 连接的网孔型网。

SDH 网络主要用作骨干网，用于连接本地网。

EPON 是一种重要的接入技术，其信号传输模式可概括为(12)。

(12)A.采用广播模式，上下行均为 CSMA/CD 方式

B.采用点到多点模式，下行为广播方式，上行为 TDMA 方式

C.采用点到点模式，上下行均为 WDM 方式

D.采用点到点模式，上下行均为 CSMA/CD 方式

【答案】B

【解析】本题考查接入网中 EPON 网的基本知识。

EPON 是第一英里以太网联盟(EFMA)在 2001 年初提出的基于以太网的无源光接入技术，IEEE802.3ah 工作小组对其进行了标准化，EPON 可以支持 1.25Gbps 对称速率，未来可升级到 10Gbps。EPON 由于其将以太网技术与 PON 技术完美结合，因此非常适合 IP 业务的宽带接入。Gbps 速率的 EPON 系统也常被称为 GE-PON。

EPON 的主要特点有：

•采用 P2MP(点到多点)传输

•单纤双向

•树型结构，ODN 可级联

•信号：下行一广播：上行一 TDMA:到达 OLT，不会到达其他的 ONU

•波长：下行一 1550nm，上行一 1310nm，采用 WDM 方式传输

•速率：1Gbps(未来 10Gbps)

甲机构构建网络时拟采用 CIDR 地址格式，其地址分配模式是 210.1.1.0/24，则实际允许的主机数最大为(13)。如果乙机构采用的地址分配模式是 210.1.0.0/16，对于目的地址为 210.1.1.10 的数据分组，将被转发到的位置是(14)。

(13)A.224　　B.28　　C.224-2　　D.28-2

(14)A.甲机构的网络　　B.乙机构的网络

C.不确定　　D.甲、乙之外的一个网络

【答案】D　A

【解析】本题考查 IP 地址，特别是 CIDR 地址格式的基本知识。

CIDR(Classless Inter-Domain Routing)将 IP 地址看成两级结构，用“IP 首地址/网络前缀位数”的形式表示。在一个网络内表示主机的地址位数为 32-网络前缀位数。全 0 和全 1 的地址不能作为普通地址分配。

对于 CIDR 格式的 IP 地址，在进行路由选择时遵循的原则是最长匹配，即选择路由表中网络前缀部分与分组中 IP 地址前缀部分的相同部分最长的那个地址作为转发地址。

IPv6 地址分为 3 级，其中第 1 级表示的含义是(15)。

(15)A.全球共知的公共拓扑　　B.本地网络　　C.网络接口　　D.保留

【答案】A

【解析】本题考查 IPv6 的基本内容。

IPv6 地址通常分为 3 级，第一级为公共拓扑，表示多个 ISP 的集合；第二级为站点拓扑，表示一个机构内部子网的层次结构；第三级唯一标识一个接口。

关于 ARP 协议，描述正确的是(16)。

(16)A.源主机广播一个包含MAC地址的报文，对应主机回送IP地址

B.源主机广播一个包含IP地址的报文，对应主机回送MAC地址

C.源主机发送一个包含MAC地址的报文，ARP服务器回送IP地址

D.源主机发送一个包含IP地址的报文，ARP服务器回送MAC地址

【答案】B

【解析】本题考查ARP协议的基本内容。

ARP协议的功能是通过已知的IP地址找到对应的MAC地址，其基本方法是：当需要获取MAC地址时，就广播一个包含IP地址的消息，收到该消息的每台计算机根据自己的IP地址确定是否应答该消息。若是被询问的机器，则发送一个应答消息，将自己的MAC地址置于其中，否则不作应答。每个机器就只需记住自身的IP地址，且该地址可动态改变。

RIP协议根据从邻居节点收到的路由信息更新自身的路由表，其更新算法的一个重要步骤是将收到的路由信息中的距离改为(17)。

(17)A.∞ B.0 C.15 D.原值加1

【答案】D

【解析】本题考查有关RIP协议的基本知识。

RIP协议更新路由的算法如下：

(1)收到相邻路由器X的RIP报文，为方便，将其称为路由表X(一个临时表)》将路由表X中“下一跳路由器地址”字段都改为X，将所有“距离”都加1(含义是：假定本路由器的下一跳为X，原来从X到达的网络的距离加上从本路由器到X的距离)；

(2)对修改后的路由表X的每一行，重复：

若目的网络不在本地路由表中，则将该行添加到本地路由表中；

否则，若下一跳的内容与本地路由表中的相同，则替换本地路由表中的对应行；

否则，若该行的“距离”小于本地路由表中相应行的“距离”，则用该行更新本地路由表中的相应行；

否则，返回；

(3)若180秒未收到邻居X的路由表，则将到邻居路由器X的距离置为16。

TCP协议在工作过程中存在死锁的可能，其发生的原因是(18)，解决方法是(19)。

(18)A.多个进程请求未被释放的资源

B.一个连接还未释放，又请求新的连接

C.接收方发送0窗口的应答报文后，所发送的非0窗口应答报文丢失

D.定义RTT值为2倍的测量值不恰当

(19)A.禁止请求未被释放的资源　　B.在一个连接释放之前,不允许建立新的连接

C.修改RTT的计算公式　　D.设置计时器，计时满后发探测报文

【答案】C　D

【解析】本题考查TCP协议的基本知识。

TCP协议在工作过程中可能发送死锁的原因是：接收方为暂缓接收数据而向发送方发送窗口为0的应答报文，发送方收到后暂停发送，等待接收到非0窗口的应答报文后继续发送新的报文。如果接收方在发送0窗口的应答报文后，所发送的非0窗口应答报文丢失，则发送方会一直等待下去。解决这一问题的方法是：发送方设置计时器，在收到0窗口应答报文后启动计时，计时满后向接收方发探测报文，提醒接收方重发非0窗口的应答报文。

FTP需要建立两个连接，当工作于Passive模式时，其数据连接的端口号是(20)。

(20)A.20　B.21　C.由用户确定的一个整数　D.由服务器确定的一个整数

【答案】D

【解析】本题考查FTP协议的基本知识。

FTP支持两种模式，一种叫做Standard(也就是PORT方式，主动方式)，一种叫Passive(也就是PASV，被动方式)。

(1)Standard模式(PORT模式)

Standard模式是FTP的客户端发送PORT命令到FTP服务器。FTP客户端首先和FTP服务器的TCP21端口建立连接，通过这个连接发送命令，客户端需要接收数据的时候在这个连接上发送PORT命令，其中包含了客户端用于接收数据的端口。服务器端通过自己的TCP20端口连接至客户端指定的端口建立数据连接发送数据。

(2)Passive模式(PASV模式)

Passive模式是FTP的客户端发送PASV命令到FTP服务器。在建立控制连接的时候和Standard模式类似，但建立连接后发送的不是PORT命令，而是PASV命令。FTP服务器收到PASV命令后，随机打开一个高端端口(端口号大于1024)并且通知客户端在这个端口上传送数据，客户端连接FTP服务器此端口(非20)建立数据连接进行数据的传送。

DNS 通常会为域名设定一个有效期(时间长度)。如果要使域名永久有效，则有效期的值应设为(21)。

(21)A.0 B.65535 C.86400 D.4294967295(即 232-1)

【答案】C

【解析】本题考查 DNS 的基本知识。

DNS 规定，域名的有效时间以秒为单位，用 86400 秒(24 小时)表示永久有效。

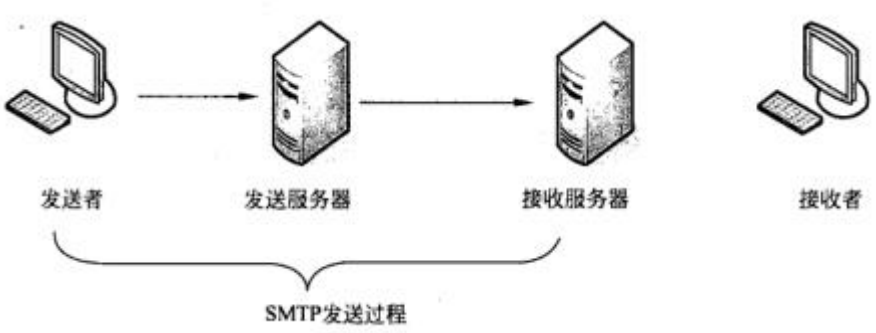
使用 SMTP 协议发送邮件时，当发送程序(用户代理)报告发送成功时，表明邮件已经被发送到(22)。

(22)A.发送服务器上 B.接收服务器上

C.接收者主机上 D.接收服务器和接收者主机上

【答案】A

【解析】本题考查 SMTP 协议的基本知识。



MIB 中的信息用 TLV 形式表示。二进制位串“110”用 TLV 形式表示时，实际占用的字节数是(23)。TLV 形式的数据被 SNMP 协议传输时，被封装成(24)进行传输。

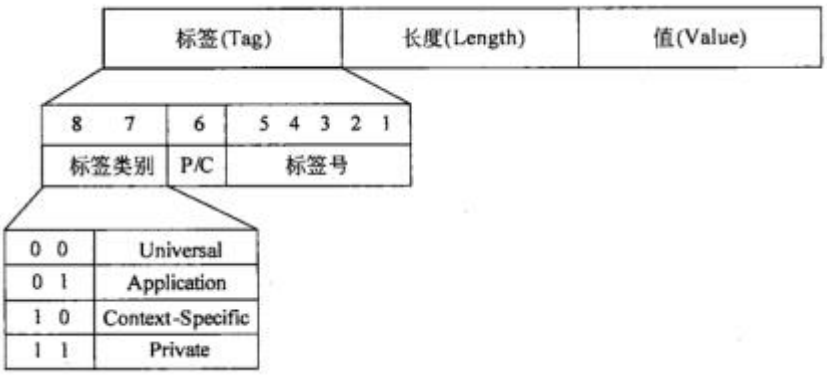
(23)A.1 B.2 C.3 D.4

(24)A.UDP 报文 B.TCP 报文 C.SMTP 报文 D.FTP 报文

【答案】D A

【解析】本题考查 ASN.1、SNMP 方面的基本知识。

MIB 中的信息用 ASN.1 规定的格式表示，每个数据由标签(Tag)、长度(Length)。值(Value)三部分外加一个可选的结束标识部分构成，如下图所示，称为 TLV 表示法。每个字段都是一个或多个字节。



IntServ 是 Internet 实现 QoS 的一种方式,它主要依靠(25),其实现资源预留的是(26)。

(25)A. SLA　　B. RSVP　　C. RTP　　D. MPLS

(26)A. 接纳控制器　　B. 调度器　　C. 分类器　　D. 路由选择协议

【答案】B　A

【解析】本题考查 QoS 及 IntServ 的基本知识。

IntServ 实现 QoS 的基本思想是，在通信开始之前利用资源预留方式为通信双方预留所需的资源，保证所需要的 QoS。

某大学拟建设无线校园网，委托甲公司承建。甲公司的张工程师带队去进行需求调研，获得的主要信息有：

校园面积约 4km2，室外绝大部分区域、主要建筑物内实现覆盖，允许同时上网用户数量为 5000 以上，非本校师生不允许自由接入，主要业务类型为上网浏览、电子邮件、FTP、QQ 等，后端与现有校园网相连，网络建设周期为 6 个月。

张工据此撰写了需求分析报告，其中最关键的部分应是(27)。为此，张工在需求报告中将会详细地给出(28)。

张工随后提交了逻辑网络设计方案，其核心内容包括：

①网络拓扑设计

②无线网络设计

③安全接入方案设计

④地址分配方案设计

⑤应用功能配置方案设计

针对无线网络的选型，最可能的方案是(29)。

针对室外供电问题，最可能的方案是(30)。

针对安全接入问题，最可能的方案是(31)。

张工在之前两份报告的基础上，完成了物理网络设计报告，其核心内容包括：

①物理拓扑及线路设计

②设备选型方案

在物理拓扑及线路设计部分，由于某些位置远离原校园网，张工最可能的建议是(32)。在设备选型部分，针对学校的特点，张工最可能的建议是(33)。

(27)A.高带宽以满足大量用户同时接入　　B.设备数量及优化布局以实现全覆盖

C.安全隔离措施以阻止非法用户接入　　D.应用软件配置以满足应用需求

(28)A.校园地图及无线网络覆盖区域示意图　B.访问控制建议方案

C.应购置或配置的应用软件清单　　D.对原校园网改造的建议方案

(29)A.采用基于 WLAN 的技术建设无线校园网

B.采用基于固定 WiMAX 的技术建设无线校园网

C.直接利用电信运营商的 3G 系统

D.暂缓执行，等待移动 WiMAX 成熟并商用

(30)A.采用太阳能供电　　B.地下埋设专用供电电缆

C.高空架设专用供电电缆　　D.以 PoE 方式供电

(31)A.通过 MAC 地址认证　　B.通过 IP 地址认证

C.在应用层通过用户名与密码认证　　D.通过用户的物理位置认证

(32)A.采用单模光纤及对应光端设备连接无线接入设备

B.采用多模光纤及对应光端设备连接无线接入设备

C.修改无线接入设备的位置，以利用 UTP 连接无线接入设备

D.将无线接入设备设置为 Mesh 和 Adhoc 工作模式，实现中继接入

(33)A.采用基于 802.11n 的高性价比胖 AP　B.采用基于 802.11n 的高性价比瘦 AP

C.采用基于 3G 的高性价比设备　　D.采用基于 LTE 的高性价比设备

【答案】B　A　A　D　C　A　B

【解析】本题考查逻网络需求设计、逻辑网络设计、物理网络设计的相关知识。

从用户的主要需求可以看出，该无线网络覆盖范围较大、用户数量多，其应用类型为普通应用。因此应重点关注设备数量及优化布局以实现全覆盖的问题，在需求报告中应给出校园地图及无线网络覆盖区域示意图。

综合现有技术成熟度及其普及程度、性能、成本等因素，WLAN 技术应是首选方案，其室外 AP 应首选 PoE 方式以减少供电线路。

因用户数量多且变化频繁、流动性强，采用应用层认证接入应是最佳的方案。

因 AP 较多且很多 AP 在室外，为方便管理，性能高的 AP 应是首选方案。

工程师利用测试设备对某信息点已经连接好的网线进行测试时，发现有 4 根线不通，但计算机仍然能利用该网线连接上网。则不通的 4 根线可能是(34)。某些交换机级联时，需要交换 UTP一端的线序，其规则是(35)，对变更了线序的 UTP，最直接的测试方式是(36)。

(34)A.1-2-3-4　　B.5-6-7-8　　C.1-2-3-6　　D.4-5-7-8

(35)A.1↔2，3↔4　　B.1↔2，3↔6　　C.1↔3，2↔6　　D.5↔6,7↔8

(36)A.采用同样的测试设备测试　　B.利用万用电表测试

C.一端连接计算机测试　　D.串联成一根线测试

【答案】D　C　B

【解析】本题考查网络布线与测试方面的基本知识。

根据相关标准,10Mbps 以太网只使用 4 根线,UTP 电缆中的 1-2-3-6 这 4 根线是必须的，分别配对成发送和接收信道。具体规定为：1、2 线用于发送，3、6 线用于接收。

当需要交换线序时，将线的其中一端的 1↔3，2↔6 分别对调。

对变更了线序的 UTP 进行测试时，最简单的方法是利用万用表测试。

某楼层的无线路由器通过 UTP 连接至网络中心，并被配置了固定的合法地址，该楼层的计算机借助该无线路由器以无线方式访问 Internet。该楼层的计算机不定期地出现不能连接到 Internet 的情况，此时，在网络中心测试该无线路由器，显示一切正常。更换同型号的无线路由器后，仍然出现上述现象。每次只要重启无线路由器，则一切恢复正常。导致这一现象的最可能原因是(37)。

(37)A.设备故障　　B.设置不当　　C.无线信号干扰　　D.网络攻击

【答案】D

【解析】本题考查网络故障分析与处理方面的基本知识。

针对本题的现象，说明有线线路、所有网络设备、用户计算机等都应该没有问题。最可能的原因应是针对 AP 的攻击导致的。

评估网络的核心路由器性能时，通常最关心的指标是(38)，与该参数密切相关的参数或项目是(39)。

(38)A.Mpps 值　　B.Mbps 值　　C.可管理 MAC 地址数　D.允许的 VLAN 数

(39)A.传输介质及数据率　　B.协议种类

C.背板交换速度　　D.内存容量及 CPU 主频

【答案】A　C

【解析】本题考查网络性能评估方面的基本知识。

对路由器，最重要的性能指标之一是单位时间内能转发的分组数，即 Mpps 值(每秒百万分组数)，其保证条件之一是背板交换速度。

张工应邀为一炼钢厂的中心机房设计设备方案。其现状是：机房处于车间附近，车间具有很高的温度，所用设备具有很强的交流电流；控制系统基于计算机网络实现数据传输、存储；约有 2000 个监测点(通过多台 PLC 设备实现)，每个监测点每 2ms 取样一次 4 字节的监测数据，通过网络发送到网络中心，并以文件形式被保存到文件服务器上，所有监测数据需在服务器上保存半年以上；对各种设备的控制信号通过同一网络传输到各监控点上；各种监测数据可在异地通过公用网络同步查看并进行实时分析。张工的方案中，将设备分为三类：一是服务器类，设计了文件服务器、数据库服务器、控制服务器、监控服务器等 4 个主要服务器；二是网络设备类，设计了一个路由器、5 台千兆交换机等主要设备；三是辅助类，包括 UPS、机房监控系统、空调等主要设备，另外计划配置有关软件系统。

文件服务器采用RAID5冗余模式、容量为1TB的硬盘构建，则应配置的硬盘数至少为(40)，优先采用的结构是(41)。

监控服务器负责接收、处理监测数据，其恰当的机型是(42)。

所配置的监测数据分析软件应具备的最基本功能是(43) 。

交换机最必要的配置是(44)。

根据上述需求，至少应增加的一台设备是(45)。

(40)A.65	B.78	C.86	D.96
(41)A.IPSAN	B.FCSAN	C.NAS	D.DAS
(42)A.大规模 Cluster	B.小规模 Cluste	C.大规模 SMP	D.小规模 SMP
(43)A.FFT 变换	B.趋势图显示	C.带通滤波	D.3D 图形
(44)A.双电源	B.光纤模块	C.VLAN 功能	D.ACL 功能

(45)A.防火墙　　B.IPS　　C.Web 服务器　　D.FTP 服务器

【答案】D C D B B A

【解析】本题考查重要的网络资源设备及机房设计的有关知识。

文件服务器的硬盘容量的最低需求为能存储半年的数据：183(天)×86400(秒/天)×500(次采样/秒)×4(B/次采样)×2000≈63TB。应该将磁盘作为文件服务器的附属存储设备，因此首选 NAS 结构。

监控服务器负责接收、处理监测数据，选用小规模 SMP 就能满足要求。

对实时数据监测的最重要功能之一是监测其变化趋势，因此趋势图分析是必不可少的。因数据的实时性要求很高，且工作环境电磁干扰严重，因此应首选光纤作为信号传输介质。由于允许其他用户通过 internet 访问监测数据，因此必须提供最基本的安全保证，而防火墙可限制非法用户访问。

主动防御是新型的杀病毒技术，其原理是(46)。

(46)A.根据特定的指令串识别病毒程序并阻止其运行

B.根据特定的标志识别病毒程序并阻止其运行

C.根据特定的行为识别病毒程序并阻止其运行

D.根据特定的程序结构识别病毒程序并阻止其运行

【答案】C

【解析】本题考查病毒与木马的基本概念。

主动防御技术是根据特定行为判断程序是否为病毒。

一些病毒程序如 CIH 声称能破坏计算机的硬件，使得计算机彻底瘫痪。其原理是(47)。

(47)A.生成高电压烧坏器件　　B.生成大电流烧坏器件

C.毁坏 ROMBIOS 程序　　D.毁坏 CMOS 中的内容

【答案】D

【解析】本题考查病毒的基本概念。

通常，病毒程序并不能毁坏硬件本身，只是破坏硬件中的软件。

IDS 是一类重要的安全技术，其实现安全的基本思想是(48)，与其他网络安全技术相比，IDS 的最大特点是(49)。

(48)A.过滤特定来源的数据包　　B.过滤发往特定对象的数据包

C.利用网闸等隔离措施　　D.通过网络行为判断是否安全

(49)A.准确度高　　B.防木马效果最好

C.能发现内部误操作　　D.能实现访问控制

【答案】D　C

【解析】本题考查 IDS 的基本知识。

IDS 的基本原理是通过分析网络行为(访问方式、访问量、与历史访问规律的差异等)判断网络是否被攻击及何种攻击。但这种分析并不能知道用户的各种突发性和变化的需求，因此很容易出现误判，并且对网络内部的误操作不能准确判断。

很多系统在登录时都要求用户输入以图片形式显示的一个字符串，其作用是(50)。

(50)A.阻止没有键盘的用户登录　　B.欺骗非法用户

C.防止用户利用程序自动登录　　D.限制登录次数

【答案】C

【解析】本题考查加密与认证的基本方法。

很多系统在登录时都要求用户输入以图片形式显示的一个字符串，可防止非法用户利用程序自动生成密码登录，即用暴力方式破解密码。

椭圆曲线密码 ECC 是一种公开密钥加密算法体制，其密码由六元组 T=<p，a，b，G，n，h>表示。用户的私钥 d 的取值为(51)，公钥 Q 的取值为(52)。

利用 ECC 实现数字签名与利用 RSA 实现数字签名的主要区别是(53)。

(51)A.0～n-1 间的随机数　　B.0～n-1 间的一个素数

C.0～p-1 间的一个随机数　　D.0～p-1 间的一个素数

(52)A.Q=dG　　B.Q=ph　　C.Q=abG　　D.Q=hnG

(53)A.ECC 签名后的内容中没有原文，而 RSA 签名后的内容中包含原文

B.ECC 签名后的内容中包含原文，而 RSA 签名后的内容中没有原文

C.ECC 签名需要使用自己的公钥，而 RSA 签名需要使用对方的公钥

D.ECC 验证签名需要使用自己的私钥，而 RSA 验证签名需要使用对方的公钥

【答案】A　A　B

【解析】本题考查椭圆曲线密码 ECC 的基本知识。

ECC 规定用户的私钥 d 为一个随机数，取值范围为 0～n-1。公钥 Q 通过 dG 进行计算(通过 Q 反算 d 是不可行的)。

RSA 实现签名的原理是分别利用自己的私钥和对方的公钥加密，签名后的内容是加密后的密文。而 ECC 的签名原理是利用密钥生成两个数附加在原始明文后一同发送。

用于保护通信过程的初级密钥在分配和传输过程中通常的形式是(54)，利用其加密或解密时，应实施的操作是(55)。

(54)A.一次一密的明文　　B.一次一密的密文

C.可多次使用的密文　　D.不限次数的密文

(55)A.利用二级密钥解密出原始密钥　　B.利用主密钥解密出原始密钥

C.利用二级密钥和主密钥解密出原始密钥　　D.利用自身私钥解密出原始密钥

【答案】A　A

【解析】本题考查密钥管理的基本知识。

初级密钥是最低级的密钥，为提高其安全性，通常采用一次一密的传送方式，即一个密钥只能使用一次，且需高一级密钥对其解密后才能用于解密。

利用交换机的 ACL 功能可增强网络的安全性和功能，其中不能实现的功能是(56)，交换机上的 RADIUS 不能实现的功能是(57)。

(56)A.限制每个端口的数据率　　B.限制每个端口的流量

C.限制每个端口可接入的 IP 地址　　D.限制每个端口可接入的 MAC 地址

(57)A.用户名认证　　B.用户密码认证　　C.用户接入权限认证　　D.流量控制

【答案】B　D

【解析】本题考查访问控制的基本知识。

ACL 是新型交换机具有的、实现访问控制的功能，具有限制每个端口的数据率、限制每个端口可接入的 IP 地址、限制每个端口可接入的 MAC 地址等很多功能，但一般都不能限制每个端口的流量。

交换机的 RADIUS 可实现安全访问控制，不对流量进行控制。

种植、自启动、隐藏是木马程序的三大关键技术。由于杀病毒软件的存在，隐秘种植木马并不容易，其中一种较好的方法是(58)。在 Windows 系统中，为实现木马的自动启动，通

常的方法是将其放于(59)中。为避免用户发现木马的存在，较好的隐藏方法(60)。

(58)A.当用户不在现场时派人安装　　B.当用户下载合法软件时顺便下载并安装

C.当用户在线观看电影时下载并安装　D.当用户打开邮件附件时安装

(59)A.autoexec.bat 文件　　B.boot.ini 文件　　C.config.sys 文件　　D.注册表

(60)A.不显示自己的名称等信息

B.把自己更名成操作系统中一个合法程序的名字

C.伪装成一个系统服务

D.需要运行时启动，运行完后退出

【答案】B　D　D

【解析】本题考查有关木马的基本知识。

为防止服务器遭攻击，通常设置一个 DMZ。有关外网、DMZ、内网三者之间的关系，应满足(61)。如果在 DMZ 中没有(62)，则访问规则可更简单。

(61)A.外网可访问 DMZ，不能访问内网，DMZ 可访问内网和外网，内网可访问外网和 DMZ

B.外网可访问 DMZ，可有条件访问内网，DMZ 可访问内网，不能访问外网，内网可访问 DMZ，不能访问外网

C.外网可访问 DMZ，不能访问内网，DMZ 可访问外网，不能访问内网，内网可访问 DMZ 和外网

D.外网可访问 DMZ，不能访问内网，DMZ 不能访问内网和外网，内网可有条件地访问 DMZ 和外网

(62)A.邮件服务器　　B.Web 服务器　　C.DNS 服务器　　D.数据库服务器

【答案】C　A

【解析】本题考查网络隔离与 DMZ 方面的基本知识。

DMZ 通常是内网服务器的一个代理，用于替代内网服务器供外网用户访问，使得内网服务器不暴露给外网用户。一旦 DMZ 中的服务器被攻击导致失效，可利用内网服务器快速恢复。邮件服务器是内外网用户都要访问的服务器，当 DMZ 中没有邮件服务器时，可以完全限制 DMZ 与内网之间的联系，只允许内网到 DMZ 的单向访问，内网安全性进一步提尚。

高速、移动是未来计算机网络的重要特征，可作为未来无线广域网络技术的是(63)，其下行、上行的数据率将分别达到(64)。

(63)A.3G B.WiMAX C.LTE D.UWB

(64)A.14.4Mbps、7.2Mbps B.52Mbps、26Mbps

C.100Mbps、100Mbps D.326Mbps、86Mbps

【答案】C D

【解析】本题考查广域网的基本知识。

LTE 即长期演进计划，是 3G 之后的下一代高速无线广域网技术，按现有技术规范，其上行、下行的数据率将分别达到 86Mbps 和 326Mbps。随着技术的进步，该数据率一定会被突破。

在项目施工前，首先要做一个进度计划，其中进度计划最常见的表示形式是(65)。

(65)A.甘特图 B.Excel 表 C.日历表 D.柱状图

【答案】A

【解析】本题考查项目管理中的进度控制的基本知识。

甘特图是进行进度管理的最常用的工具，其通常形式是纵向表示项目，横向表示所需的时间。几乎所有的 IT 项目管理软件都具有甘特图功能。

网络工程项目质量管理的重要标准是(66)。

(66)A.CMM B.GB 8567 C.ISO 9001 D.ISO 14000

【答案】C

【解析】本题考查质量管理标准方面的基本知识。

ISO 9001 是重要的质量管理标准。ISO 9001 对设计开发到生产、安装及服务等全过程提出了要求。

CMM(软件成熟度模型)是关于软件开发管理的一个模型，GB 8567 是中国关于软件开发过程的一个国家标准，主要是文档制作规范，ISO 14000 是环境管理系列标准。

乙公司中标承接了甲机构的网络工程集成项目，在合同中约定了因不可抗力因素导致工期延误而免责的条款，其中不被甲机构认可的一种因素是(67)。合同约定，甲乙双方一旦出现分歧，在协商不成时，可提交到相关机构裁定，一般优先选择的裁定机构是(68)。

(67)A.施工现场遭遇长时间雷雨天气 B.物流公司车辆遭遇车祸

C.乙方施工队领导遭遇意外情况 D.甲机构相关负责人变更

(68)A.甲机构所在地的仲裁委员会　　B.乙公司所在地的仲裁委员会

C.甲机构所在地的人民法院　　D.乙公司所在地的人民法院

【答案】C　A

【解析】本题考查项目管理中合同制定与管理方面的基本知识。

不可抗力因素通常是指自然、环境或不可控制的第三方因素，乙方自身的因素应是可控因素，一般都不会被认同为不可抗力因素。

当发生分歧且协商不成时，一般情况下都是优先选择仲裁机构裁决，这样便于双方进一步协商且有利于控制矛盾升级。

在市场经济条件下，因甲方通常具有主动权，所以一般选择甲方所在地的仲裁委员会或法院。

甲公司委托销售部的客户经理张经理代表公司参加一个网络工程项目的投标，张经理在规定时间内提交了投标文件招标单位在详细审查了投标文件后向张经理提出了一个简单的问题：你是甲公司的代表吗？张经理于是赶紧找到招标单位的王科长作证，以证明他是甲公司的。对甲公司的此次投标，最可能的结果是(69)。

(69)A.因在招标单位有重要的熟人而顺利入围进入下一轮

B.因张经理没有书面授权而无法通过资格审查被淘汰

C.因通过补交证明材料顺利进入下一轮

D.因甲公司法人代表随后赶到参与答辩而顺利进入下一轮

【答案】B

【解析】本题考查项目管理中招投标方面的基本知识。

按招标文件要求提交具有授权、公司盖章的各种书面材料是投标的唯一合法材料，依靠熟人作证不能作为有法律效力的证明材料。

M/M/1 排队论模型是分析网络性能的重要工具，假定通信量强度为ρ(信道的平均繁忙程度)，则节点中的等待输出的平均分组数为(70)。

(70)A.1/(1-ρ)　　B.ρ/(1-ρ)　　C.(1-ρ)/ρ　　D.ρ

【答案】B

【解析】本题考查排队论的应用。

排队论是分析网络性能最重要的工具之一。

A Bluetooth device can be either a master or a slave and any of the devices within a(71)can be the master. There is only one master and there can be up to (72) active slave devices at a time within a single network. In addition, a device may be a standby slave or a parked slave. There can be up to (73) parked slaves. If there are already maximum number of active slaves, then a parked slave must wait until one of the active slaves switches to (74) mode before it can become active. Within a network, all (75) communications are prohibited.

(71)A.Wireless LAN　　B.Wireless MAN

C.Cellular radio network　　D.Piconet

(72)A.7　　B.15　　C.63　　D.255

(73)A.127　　B.255　　C.511　　D.1023

(74)A. master　　B.standby slave

C.parked slave　　D.active slave

(75)A.master-to-master　　B.master-to-slave

C.slave-to-slave　　D.master-to-master

【答案】D　A　B　C　C

【解析】

蓝牙设备可以是一个主设备，也可以是一个从设备，位于(71)中的任一设备都可以成为主设备。在一个网络中只有一个主设备，最多有(72)个激活的从设备。另外，一个设备可以是活跃的从设备或是休眠的从设备，最多有(73)个休眠的从设备。如果已有最大数量的活跃从设备，那么，一个休眠的从设备就必须等到某活跃从设备切换到(74)模式后才能被激活。在一个网络内，所有的(75)通信都是被禁止的。

试题一

某省准备建立电子政务网络平台，实现全省上下各级部门之间的信息交换和资源共享。遵照《国家信息化领导小组关于推进国家电子政务网络建设的意见》的要求，电子政务网络分为电子政务外网和电子政务内网，该省即将建设的网络平台被定性为“非涉密”的电子政务外网。在第一期工程中，主要建设覆盖省直部 R 和各地市州的电子政务外网省级部分。电子政务外网是办公自动化、会议通知、行政审批、电子监察等跨部门应用系统的运行网络，还是一个网络承载平台，可以承载各类 VPN。例如，在当前的省级外网平台建设中，外网平台就需要承载两个 VPN:(1)互连各个部门的国库支付 VPN;(2)互连各个部门的视频监控 VPN。

【问题 1】

电子政务外网承载 VPN，可以采用 L2TP、IPSec、MPLS VPN 三类技术，请对三种技术建设 VPN 进行比较，比较内容如表 1-1 所示。

表 1-1 VPN 技术比较

比 较 项 目	L2TP	MPLS VPN	IPSec	备 注
隧道协议层次				对隧道的协议层次进行比较
是否支持数据加密				
设备的要求				比较网络核心、边缘设备的协议支持要求
是否支持移动 VPN 客户端				

比较项目	L2TP	MPLS VPN	IPSec	备 注
隧道协议层次	第二层	介于第二层和第三层之间（或两层半）	第三层	对隧道的协议层次进行比较
是否支持数据加密	不支持	不支持	支持	
设备的协议支持要求	只要求边缘设备支持 L2TP	要求边缘和核心设备都支持 MPLS	只要求边缘设备支持 IPSec	比较网络核心、边缘设备的协议支持要求
是否支持移动 VPN 客户端	支持	不支持	支持	

本题涉及 MPLS 技术、MPLS VPN 等领域的内容。

VPN(Virtual Private Network，虚拟专用网)就是利用 Intemet 或其他公共互联网络的基础设施建立专用数据传输通道，将远程的分支机构、移动办公人员等连接起来，实现不同网络的组件和资源之间的相互连接，是通过隧道技术在公共数据网络上虚拟出一条点到点的专线技术。

在虚拟专用网中，任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，

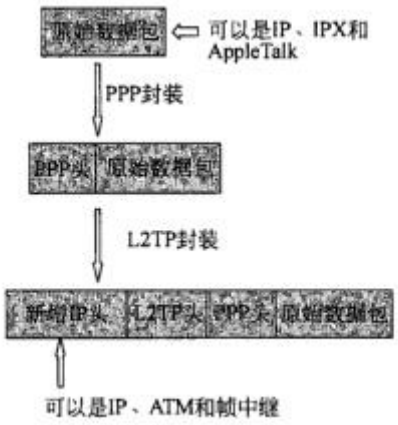
而是利用某种公众网的资源动态组成的。

VPN 主要采用 4 项技术来保证安全，这 4 项技术分别为隧道技术(Tunneling)、加解密技术(Encryption & Decryption)、密钥管理技术(Key Management)、认证技术(Authentication)。

隧道技术就是利用隧道协议对隧道两端的数据进行封装的技术。利用一种协议来传输另外一种协议的技术，共涉及三种协议，包括乘客协议、隧道协议和承载协议，隧道协议可以分别是第二层或第三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中，再把整个数据包装入随道协议中；这种双层封装方法形成的数据包靠第二层协议进行传输；第二层随道协议有 L2F、PPTP、L2TP 等。第三层隧道协议则借助于网络层协议来进行封装，典型代表是 IPSec；IPSec 本身不是隧道协议，但由于其提供的认证、加密功能适用于建立 VPN 环境，它既能提供 LAN 间 VPN，也能提供远程访问型 VPN。而 MPLS VPN 则是一种借助于标签交换技术、利用公用 MPLS 基础设施实现多个用户网络承载，是一种介于第二层和第三层之间的技术。

L2TP 协议：

L2TP 封装的乘客协议是位于第二层的 PPP 协议，如下图所示。



L2TP 在数据传输过程中并没有对数据进行加密。

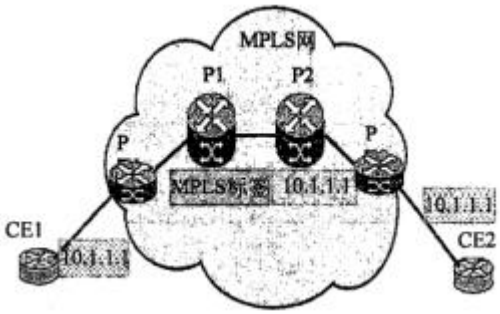
IPSec 协议：

IPSec 只能工作在 IP 层，要求乘客协议和承载协议都是 IP 协议，如下图所示。

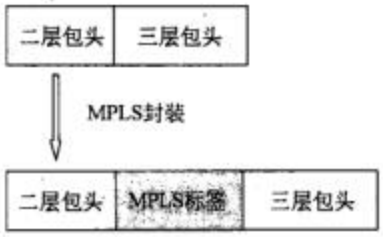
IPSec 在传输数据过程中，可以对被封装的数据包进行加密和摘要等，以进一步提高数据传输的安全性。

MPLS VPN：

MPLS VPN 技术借助于一个公用的 MPLS 域，在入口边缘路由器为每个包加上 MPLS 标签，核心路由器根据标签值进行转发，出口边缘路由器再去掉标签，恢复原来的 IP 包，如下图所示。



MPLS 标签位于二层和三层之间，其协议封装如下图所示。



【问题 2】

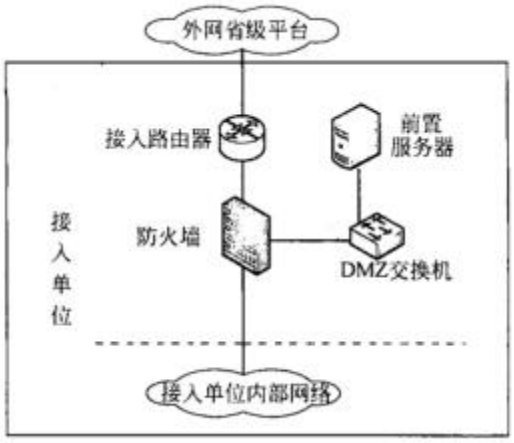
各地市州、各省直部门在接入电子政务外网平台时，需要配置接入路由器、防火墙、前置服务器，请考虑如下连接要求，并添加相应的连接线路或设备，给出接入电子政务外网的设备连接图。

(1)部门网络与电子政务外网之间为逻辑隔离；

(2)部门应用系统主动把数据推送至前置服务器，数据中心在进行数据获取时，不允许进入部门网络；

(3)在调试防火墙的各类过滤规则时，不会对电子政务外网的路由造成影响；

(4)可根据用户负载的需要，随时添置前置服务器。



画图要点：

接入路由器直接连接电子政务外网；

防火墙直接连接单位内部网络；

防火墙与接入路由器直接相连；

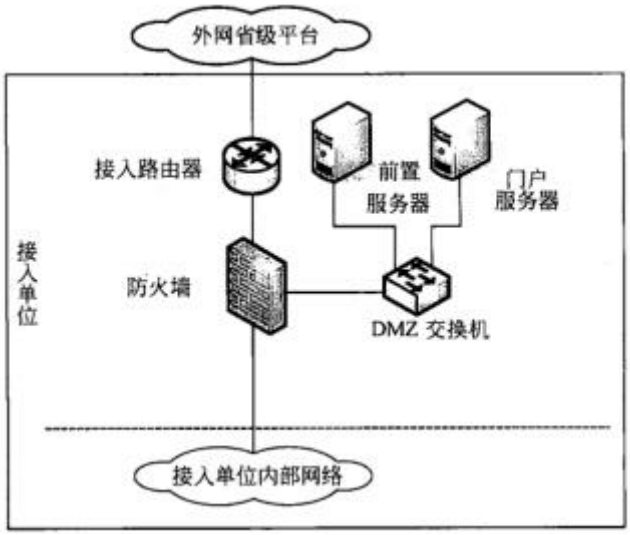
防火墙的 DMZ 口添置一台 DMZ 交换机；

前置服务器与 DMZ 交换机直接相连。

电子政务网络一般分为电子政务内网和电子政务外网。其中电子政务外网是一个非涉密性质的网络，可以借助于特定的安全手段，实现普通信息和敏感信息的传递。电子政务外网在实现部门和下级单位接入时，主要采用逻辑隔离方式接入，即指两个网络之间存在着受控的网络协议传递，信息借助于防火墙或者具有过滤功能的路由器实现交换的方式。

逻辑隔离接入方式适用于大多数部门，其内部网络为实现对内部信息与资源实施保护，在受控的情况下与外网进行连接。由于电子政务网络建设主要为政务信息资源目录体系、政务信息资源交换体系、各类电子政务应用系统提供运行和承载环境；在实现部门网络接入的同时，需要为信息和数据的交换提供有效的技术支撑；因此，部门网络借助于防火墙或路由器完成与电子政务外网主干的连接，通过受控的网络协议实现信息交换。

传统意义上的部门逻辑接入方式如下图所示。



为完成各部门网络接入电子政务外网平台，必须配置特定的网络接入设备，这些设备主要包括接入路由器、防火墙、前置服务器、DMZ 交换机等。

•接入路由器是实现单位接入的关键设备，通过运行路由算法，保持和外网平台的连通性。

•前置服务器是完成单位内部网络和外网平台数据交换的关键设备，通过前置数据库、交换中间件等实现数据的交换。

•防火墙是完成逻辑隔离的关键设备，其强大的过滤机制、DMZ 区域设置等技术，保证了外网平台与单位网络之间的受控信息传递。

•DMZ 交换机用于扩展防火墙的 DMZ 区域，实现多台服务器在防火墙 DMZ 区域的接入。

【问题 3】

如图 1-1 所示，省级电子政务外网平台承载了两个 VPN，分别为国库支付 VPN 和视频监控 VPN。请从以下方面描述电子政务外网 PE 路由器上的 MPLS VPN 配置内容:

•VPN 接口配置

•PE-CE 配置

•OSPF 配置

•MPLS 配置

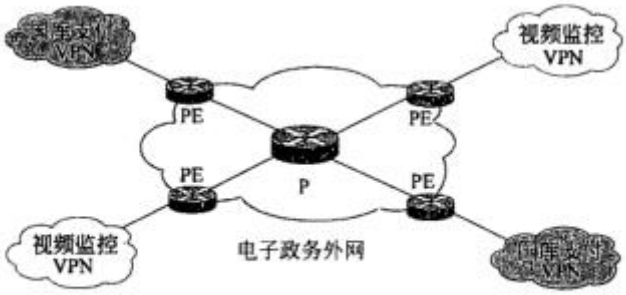


图 1-1 电子政务外网承载 VPN 示意图

(1)VPN 接口配置

将相应的接口加入 VPN 实例中；

进入接口配置模式，配置接口的 IP 地址。

(2)PE-CE 配置

启用路由协议 BGP，并设置自治区号；

在 BGP 的 IPv4VRF 实例地址簇中引入路由信息；

建立 IPv4VRF 实例的邻居关系，激活并传递 VRF 路由；

在 BGP 中引入直连路由。

(3)OSPF 配置启用 OSPF 路由协议；

配置路由区域及网络地址信息。

(4)MPLS 配置

配置 MPLS 的 LSRID 标识；

启用路由器的 MPLSLDP 标签协议；

在网络接口上启用 MPLSLDP 标签协议。

MPLS 最初是用来提高路由器的转发速度而提出的一个协议，MPLS 协议的关键是引入了标签(Label)交换概念；标签是一种短的、易于处理的、不包含拓扑信息、只具有局部意义的信息内容。

在 MPLS 网络中，IP 包在进入第一个 MPLS 设备时，MPLS 边缘路由器分析 IP 包的内容并且为这些 IP 包选择合适的标签；以后所有 MPLS 网络中的节点都是依据这个标签作为转发依据；当 IP 包最终离开 MPLS 网络时，标签被边缘路由器分离。

MPLS 在逻辑上可以分为 LER(Label Edge Router)和 LSR(Label Switching Router)。其中 LER 是 MPLS 网络同其他网络的边缘设备，它提供流量分类和标签映射、标签移除的功能；而 LSR 是 MPLS 网络的核心交换机，它提供标签交换、标签分发的功能。

作为一种高效的 IP 骨干网技术平台，MPLS 为实现 VPN 提供了一种灵活的、具有可扩展性的技术基础，并且具有网络配置简单、动态发现相邻节点、直接利用现有路由协议、具有良好的可扩展性等特点。

为支持基于 MPLS 的 VPN 特性，必须实现如下功能：

•LDP(Label Distribution Protocol)标签分布协议，是 MPLS 的信令协议，用以管理和分配标签；

•MPLS 转发模块，根据报文上的标签和本地映射表进行二、三层间交换；

•MBGP 和 BGP 扩展，用来传递 VPN 路由和承载 VPN 属性、QoS 信息、标签等内容；

•路由管理的 VPN 扩展，建立多路由表，用以支持 VPN 路由。

在 MPLSVPN 的连接模型中，网络由运营商的骨干网与用户的各个 Site 组成，所谓 VPN 就是对 Site 集合的划分，一个 VPN 就对应一个由若干 Site 组成的集合。而 MPLSVPN 网络中的路由设备也相应分为三类：

•CE(Custom Edge)：用户 Site 中直接与服务提供商相连的边缘设备；

•PE(Provider Edge)：骨干网中的边缘设备，它直接与用户的 CE 相连；

•P 路由器(Provider Router):骨干网中不与 CE 直接相连的设备。

MPLS VPN 的组成原理如下：

(1)MPLS VPN 的网络构造由服务提供商来完成。在这种网络构造中，由服务提供商向用户提供 VPN 服务，用户感觉不到公共网络的存在，就好像拥有独立的网络资源一样。

(2)同样对于服务提供商骨干网络内部的 P 路由器，也就是不与 CE 直接相连的路由器而言，也不知道有 VPN 的存在，仅仅负责骨干网内部的数据传输。但其必须能够支持 MPLS 协议，并使能该协议。

(3)所有的 VPN 的构建、连接和管理工作都是在 PE 上进行的。PE 位于服务提供商网络的边缘。从 PE 的角度来看，用户的一个连通的 IP 系统被视为一个 Site，每一个 Site 通过 CE 与 PE 相连，Site 是构成 VPN 的基本单元。

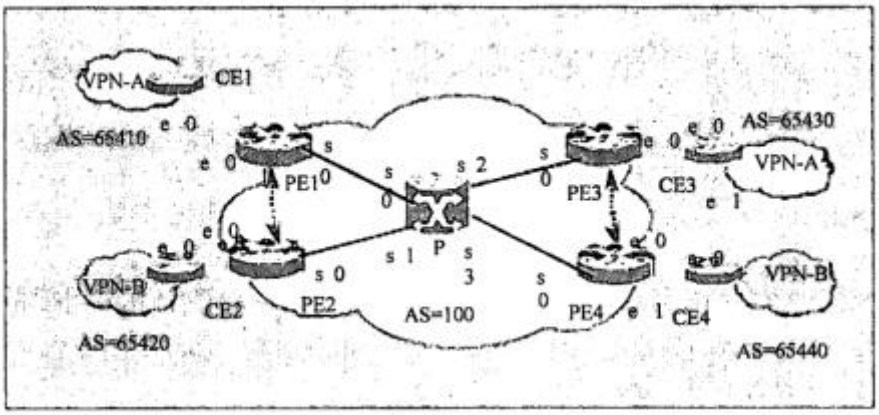
(4)一个 VPN 是由多个 Site 组成的，一个 Site 也可以同时属于不同的 VPN。属于同一个 VPN 的两个 Site 通过服务提供商的公共网络相连，VPN 数据在公共网络上传播，必须要

保证数据传输的私有性和安全性。也就是说，从属于某个 VPN 的 Site 发送出来的报文只能转发到同样属于这个 VPN 的 Site 中去，而不能被转发到其他 Site 中去。

(5)同时，任何两个没有共同的 Site 的 VPN 都可以使用重叠的地址空间，即在用户的私有网络中使用自己独立的地址空间，而不用考虑是否与其他 VPN 或公网的地址空间冲突。所有这些就都需要依赖于 VRF(VPN Routing& Forwarding Instance)。

关于 VPN 路由转发实例(VPN Routing & Forwarding Instance)、路由标识(Route Distinguisher)，多协议 BGP(Multiprotocol BGP)、BGP 扩展团体属性(Extended Community)、BGP 路由刷新(Route Refresh)的详细技术内容，在本文中不做介绍，请参阅相关技术资料。

以下为问题 3 的 MPLSVPN 环境介绍及 MPLSVPN 的有关配置。



图中，s0 表示第 0 号串口，e0 表示第 0 号以太网口；P 路由器分别通过 s0、s1、s2、s3 与 PE1、PE2、PE3、PE4 相连;各用户网络的 AS 号码分别为 65410、65420、65430、65440，核心网络的 AS 号码为 100；VPN-A 为国库支付 VPN，VPN-B 为视频监控 VPN。

PE1 的配置：

```
# VRF 配置
Quidway#config terminal
#进入到配置模式
Quidway(config)#ip vrf vpna
#创建 VPN 实例 VPNA
Quidway(config-vrf)#rd 100:1
#配置 VPNA 的 rd 为：100:1
Quidway(config-vrf)#route-target both 100:1
#配置 rd 为 100:1 的站点可以双向接收此 VPN 路由
Quidway(config-vrf)#route-target import 100:2
#可以接收到 rd 为 100:2 站点发送过来的 VPN 路由
Quidway(config-vrf)#route-target export 100:3
#配置 rd 为 100:3 的站点可以接收此 VPN 路由
Quidway(config-vrf)#exit
#退出接口配置模式

# 接口配置
Quidway(config)#interface e 0
#进入到以态网 e0 口
Quidway(config-if-Ethernet0)#ip vrf forwarding vpna
#将接口添加到 VPNA 实例中
Quidway(config-if-Ethernet0)#ip address 168.1.1.2 255.255.0.0
#配置接口地址
Quidway(config-if-Ethernet0)#exit
#退出接口配置模式
Quidway(config)#interface s 0
#进入到串行接口 s0 口
Quidway(config-if-Serial0)#ip address 172.1.1.1 255.255.0.0
#配置接口地址
Quidway(config-if-Serial0)#exit
#退出接口配置模式

# PE-CE 配置
Quidway(config)#router bgp 100
#使能 BGP，自治系统号 100
Quidway(config-router-bgp)#address-family ipv4 vrf vpna
#在 BGP 的 IPv4 VRF VPNA 地址簇中引入路由信息
Quidway(config-router-af)#neighbor 168.1.1.1 remote-as 65410
#建立 IPv4 VRF VPNA 中的邻居，传递 VRF 路由
```

```
Quidway(config-router-af)#neighbor 168.1.1.1 activate
#建立 IPv4 VRF VPNA 中的邻居，并激活邻居
Quidway(config-router-af)#redistribute connected
#引入直连路由
Quidway(config-router-af)#exit-address-family
#退出当前配置模式
Quidway(config-router-bgp)#exit
#退出

# PE-PE 配置
Quidway(config)#router bgp 100
#使能 BGP，自治系统号 100
Quidway(config-router-bgp)#redistribute ospf metric 6
#引入 OSPF 路由并配置 metric 值为 6
Quidway(config-router-bgp)#address-family vpnv4
#配置 VPNV4 iBGP 路由，用以在 PE 之间传播 MBGP VPN 路由
Quidway(config-router-af)#neighbor 172.2.1.1 remote-as 100
#建立邻居
Quidway(config-router-af)#neighbor 172.2.1.1 activate
#激活邻居
Quidway(config-router-af)#neighbor 172.3.1.1 remote-as 100
Quidway(config-router-af)#neighbor 172.3.1.1 activate
Quidway(config-router-af)#neighbor 172.4.1.1 remote-as 100
Quidway(config-router-af)#neighbor 172.4.1.1 activate
Quidway(config-router-af)#exit-address
Quidway(config-router-bgp)#exit
# OSPF 配置
Quidway(config)#router ospf
#启用 OSPF 功能


Quidway(config-router-ospf)#network 172.1.1.0 0.0.255.255 area 0
#发布 OSPF 路由信息到区域 0
Quidway(config-router-ospf)#exit
# MPLS 配置
Quidway(config)#mpls lsr id 172.1.1.1
#配置 MPLS 的 lsr id 标识
Quidway(config)#mpls ldp
#启用 MPLS LDP 标签协议
Quidway(config-mpls-ldp)#exit
Quidway(config)#interface s 0
Quidway(config-if-Serial0)#mpls ldp enable
#在接口下启用 MPLS 标签功能

    Quidway(config-if-Serial0)#exit
    Quidway(config)#exit
    Quidway#
```

CE1 的配置：

```
# 接口配置
Quidway#config terminal
Quidway(config)#interface e 0
Quidway(config-if-Ethernet0)#ip address 168.1.1.1 255.255.0.0
#配置以太口 IP 地址
Quidway(config-if-Ethernet0)#exit
# BGP 配置
Quidway(config)#router bgp 65410
Quidway(config-router-bgp)#neighbor 168.1.1.2 remote-as 100
#配置 BGP 邻居
Quidway(config-router-bgp)#exit
Quidway(config)#exit
Quidway#
```

p 路由器的配置：

```
# 接口配置
Quidway#config terminal
Quidway(config)#interface s 0
Quidway(config-if-Serial0)#ip address 172.1.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
Quidway(config)#interface s 1
Quidway(config-if-Serial0)#ip address 172.2.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
Quidway(config)#interface s 2
Quidway(config-if-Serial0)#ip address 172.3.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
Quidway(config)#interface s 3
Quidway(config-if-Serial0)#ip address 172.4.1.2 255.255.0.0
Quidway(config-if-Serial0)#exit
#配置各串口 IP 地址
# MPLS 配置
Quidway(config)#mpls lsr id 172.1.1.2
#配置 MPLS 的 lsr id 标识
Quidway(config)#mpls ldp
#启用 MPLS LDP 标签协议
```

```
Quidway(config-mpls-ldp)#exit
Quidway(config)#interface s 0
Quidway(config-if-Serial0)#mpls ldp enable
#在接口下启用 MPLS 标签功能
Quidway(config-if-Serial0)#exit
Quidway(config)#
Quidway(config)#interface s 1
Quidway(config-if-Serial0)#mpls ldp enable
Quidway(config-if-Serial0)#exit
Quidway(config)#
Quidway(config)#interface s 2
Quidway(config-if-Serial0)#mpls ldp enable
Quidway(config-if-Serial0)#exit
Quidway(config)#
Quidway(config)#interface s 3
Quidway(config-if-Serial0)#mpls ldp enable
Quidway(config-if-Serial0)#exit
Quidway(config)#
# OSPF 配置
Quidway(config)#router ospf
Quidway(config-router-ospf)#network 172.1.1.0 0.0.255.255 area 0
Quidway(config-router-ospf)#network 172.2.1.0 0.0.255.255 area 0
Quidway(config-router-ospf)#network 172.3.1.0 0.0.255.255 area 0
Quidway(config-router-ospf)#network 172.4.1.0 0.0.255.255 area 0
```

其他 PE 的配置与 PEI 相似，其他 CE 的配置与 CE1 相似，不重复列举。

试题二

长江沿线某物流企业 A 与 B 并购后组织机构合并，在此情况下，原有两个单位的信息网络的融合成为迫在眉睫的任务。在机构融合前，两个单位各自都有独立的广域网络：A 企业广域网覆盖重庆至上海，共 1 个核心节点(武汉长江南岸，100 个用户)、6 个二级节点(30 个用户)和 23 个三级节点(9 个用户)；B 企业广域网覆盖重庆至芜湖，共 1 个核心节点(武汉长江北岸，150 个用户)、11 个分支核心节点(11 个用户，包含 A 企业的二级节点)、200 多个扫描接入点(2 个终端)。两个广域网的主要传输通道都是通过 A 企业自建的 SDH 网络：A 企业广域网一二级节点间是 155MPOS 互联，二三级节点间采用 10MMSTP 或 2M 电路互联，少数链路为 40MMSTP;B 企业广域网核心和分支机构的互联采用 30～50MMSTP 互联，少数节点采用 4 个 2M 捆绑的电路连接。(注：所有 MSTP 电路使用仅用于实现二三级节点的点对点连接)

A 企业广域网承载着办公、视频监控、软交换、视频会议、广播控制系统等业务；

B 企业广域网承载着办公、视频会议、数十个安全监管业务系统、CCTV、GPS 等物流监管系统等业务系统。

机构融合后，两个广域网再没有独立运行的必要了，因此要将两个广域网合并成一个网络，清理网络资产、简化网络结构(减少二级节点数量)、优化路由，使网络安全、高效、可靠、易维护、易管理。A 企业广域网结构如图 2-1 所示。

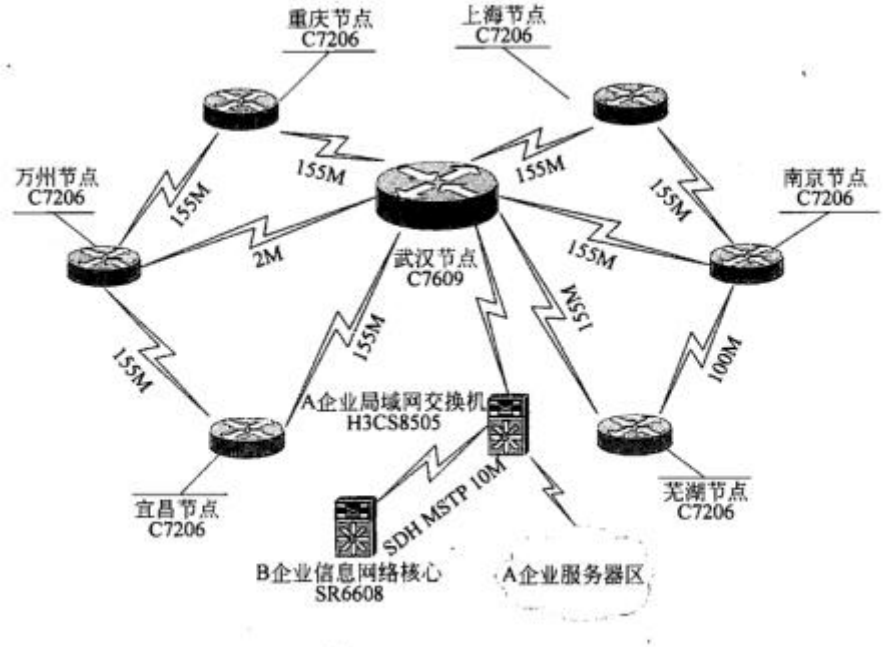


图 2-1 A 企业广域网结构

B 企业广域网结构如图 2-2 所示。

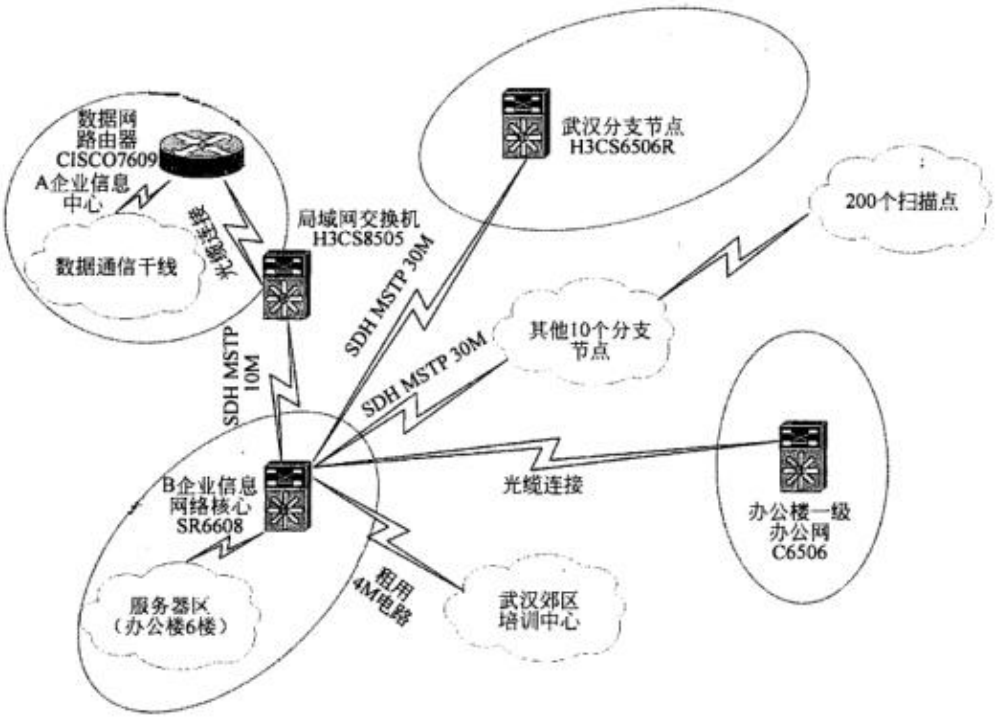


图 2-2 B 企业广域网结构

【问题 1】

在不增加新设备、新链路的情况下，针对现有物理设备及线路给出整合解决方案的整体思路。要求：

(1)整合后的企业网络采用层次化设计、简化拓扑，实现核心节点、线路 N+1 冗余；

(2)整合后企业网络的二级节点包括重庆、万州、宜昌、芜湖、南京、上海以及位于武汉的“培训中心”和“武汉分支管理处”。

解决方案的整体思路：

(1)武汉的核心路由设备迁移到一个核心机房，并迁移原有与二级设备的链路；

(2)所有服务器、核心交换机迁移到武汉的核心机房，并实现服务器区与两台核心交换机的默认网关冗余；

(3)统一采用二级、三级节点方式，打乱原有连接方式；对 8 个二级节点以外的节点都降级为三级节点；对原 A 企业三级节点、B 企业节点分扫描接入点采用就近接入原则或者就近线路迁移原则，形成三级网络结构；

(4)原有 155M 线路作主用，30M 线路作备用。

本题涉及网络升级改造、性能优化等方面的内容。

在进行企业网络整合改造之前，必须明确企业网络的现状，包括以下内容：

•待整合网络的网络结构；

•各网络节点的设备清单；

•设备接口及连接情况；

•待整合网络 IP 地址规划；

•待整合网络路由规划。

在了解了网络现状之后，应制定网络整合的整体目标，本题中网络改造的整体目标是原有长江沿线的物流企业 A 和 B 的网络合并为一个网络，建设完成一地一中心、结构层次化网络，为物流企业日常办工及各应用系统提供快捷、可靠、稳定的统一的网络平台。

为实现网络整合的整体目标，还需要对网络平台的需求进行分析，需要包括以下内容：

•业务需求分析，主要包括网络需要承载的业务系统；

•IT 资源利用分析，包括线路资源、网络设备资源、IP 地址资源；

•整合后的网络结构分析；

•整合后的网络路由规划分析；

•改造的可行性分析，包括必要性、技术可行性、风险性等。 .

基于以上分析，形成整合改造方案。在本题中，可以采用如下的整体思路：

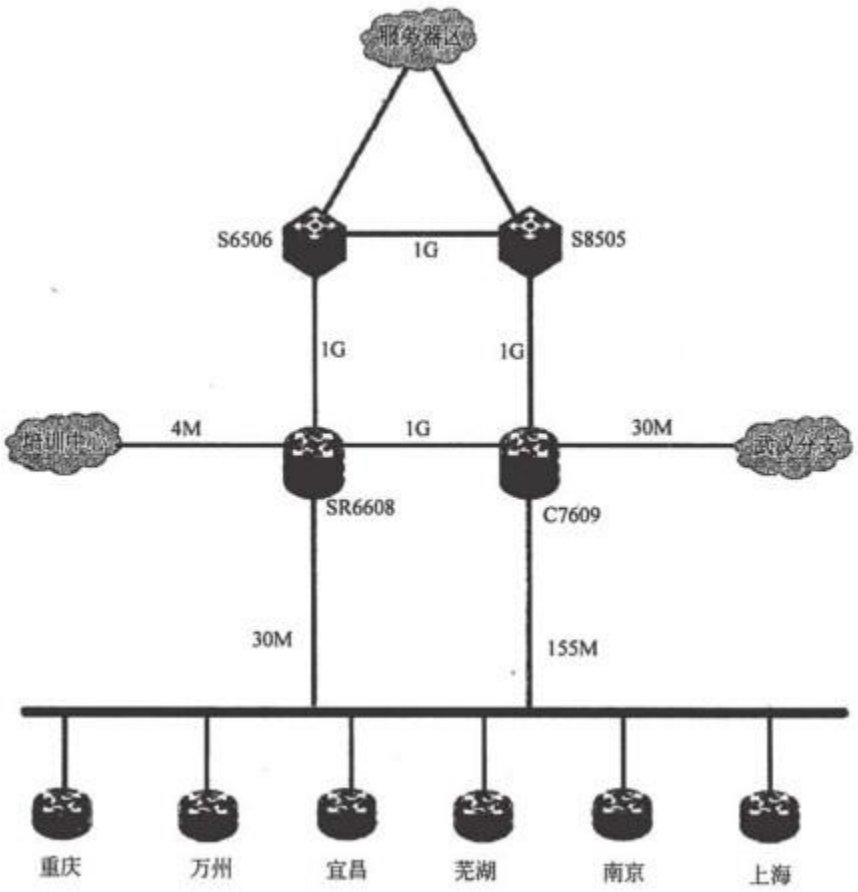
•武汉的核心路由设备迁移到一个核心机房，并迁移原有与二级设备的链路；

•所有服务器、核心交换机迁移到武汉的核心机房，并实现服务器区与两台核心交换机的默认网关冗余；

••统一采用二级、三级节点方式，打乱原有连接方式；对 8 个二级节点以外的节点都降级为三级节点；对原 A 企业三级节点、B 企业扫描接入点采用就近接入原则或者就近线路迁移原则，形成三级网络结构；

•原有 155M 线路作主用，30M 线路作备用。

最终可以形成新的网络结构，如下图所示。



【问题 2】

原 A 企业服务器地址采用 172.16.1.0/24一个 C 类地址段，原 B 企业服务器地址采用 192.168.0.0/24、192.168.1.0/24 两个 C 类地址段。A、B 两企业用户地址和网络设备地址都采用 10.0.0.0/8 地址。要求在不影响业务的情况下采用层次化的地址分配方案合理规划地址(禁止使用 NAT 技术)，并提供地址切换解决方案。

地址切换解决方案：

1.所有核心设备整合到一个机房后，在服务器区划分三个或多个 VLAN，使原有服务器网段地址不作修改，以保障业务系统的正常使用。

2.用户地址进行统一规划，采用先横向再纵向的方式对各单位进行地址分配，各单位进行地址分配时对地址进行合理预留，以满足后期扩展。并采用 DHCP 技术自动分配业务地址。

3.设备管理地址采用 32 位掩码、属于单一地址段的地址进行全网统一规划，设备互联地址采用 30 位掩码的地址进行全网统一规划。

整合改造方案中，IP 地址规划是一个关键性问题，整合后的 IP 地址规划应依据科学性、系统性、完整性及可扩展性的代码分类原则，同时还应考虑如下思路=

•IP 地址资源以地域划分、行政隶属关系和业务种类为层次，分割为大小不同、用途各异的地址块单元；

•实现地址的层次化划分，以利于路由信息的聚合，减少路由表长度；

•充分利用网络地址资源和信息资源，可根据实际需要分配地址，避免不必要的地址空间的浪费；

•地址分配应简单、易于管理，降低网络扩展的复杂性，减少路由表的路由条数；

•地址分配在每一个层次都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性；

•地址分配应具有灵活性，以满足各种路由策略的优化，充分利用地址空间；

•便于制定统一的网络管理策略，实现统一的网络管理；

•便于网络安全策略的实现；

•为不同地域间的信息交换设计出优良的稳定网络的 IP 地址编码规范；

•各局域网内不同类型的应用必须使用不同子网的 IP 地址，以便于不同的应用使用不同的路由策略。

针对 A、B 企业服务器地址段不同，但是用户地址和网络设备地址段重复的现状，可以采用如下的地址切换解决方案，以实现平滑过渡：

•所有核心设备整合到一个机房后，在服务器区划分三个或多个 VLAN，使原有服务器网段地址不作修改，以保障业务系统的正常使用；

•用户地址进行统一规划，采用先横向再纵向的方式对各单位进行地址分配，各单位进行地址分配时对地址进行合理预留，以满足后期扩展。并采用 DHCP 技术自动分配业务地址；

•设备管理地址采用 32 位掩码、属于单一地址段的地址进行全网统一规划，设备互联地址采用 30 位掩码的地址进行全网统一规划。

【问题 3】

原 A 企业采用 OSPF 作为路由协议，协议进程规划为 1，二级节点作为 area0 边界且往下分别归属于不同的 area。原 B 企业采用 OSPF 作为路由协议，协议进程规划为 10，分支节点作为 area0 边界且往下分别归属于不同的 area。合并前 A、B 两企业之间采用静态路由连接。要求提供两种基于 OSPF 协议的路由整合方案思路，并比较两种整合思路的优缺点。

路由整合方案：

路由整合方案一：整合所有路由器到一个 OSPF 体系中，所有核心设备规划到核心区域 AREA0 中，其他节点按归属划分到不同的区域中。

路由整合方案二：采用多进程 OSPF 技术，将原有两个单位的 OSPF 启用两个不同的进程，再进行路由的相互导入。

路由整合方案比较：

第一种方案较优，能使整个网络中的路由更加清晰，区域的划分更加合理，并能有效地进行路由汇总。

第二种方案通常是网络整合中的过渡性方案，实际上在网络中存在两个路由体系，借助于路由体系之间的路由引入而形成互连互通，因此形成的最短路径并不是真正意义上的最短路径，并且会影响路由收敛效率。

OSPF 支持多进程，在同一台路由器上可以运行多个不同的 OSPF 进程，它们之间互不影响，彼此独立。不同 OSPF 进程之间的路由交互相当于不同路由协议之间的路由交互。路由器的一个接口只能属于某一个 OSPF 进程。

本问题是一个较为典型的案例，待整合的网络都采用 OSPF 作为路由协议，只是 OSPF 进程号不同；在进行网络整合的路由规划时，可以采用两种思路：一是在整合后的网络中只存在一个 OSPF 体系，所有路由器都使用相同的 OSPF 进程号；二是所有路由器的原有 OSPF 进程号不发生改变，在整合后的网络中存在两个 OSPF 体系，两个 OSPF 体系之间采用路由引入，使得所有路由器之间可以互访。

试题三

某企业网络拓扑结构如图 3-1 所示。根据企业要求实现负载均衡和冗余备份，构建无阻塞高性能网络的建设原则，该企业网络采用两台 S7606 万兆骨干路由交换机作为双核心，部门交换机 S2924G 通过光纤分别与两台核心交换机相连，通过防火墙和边界路由器与 Internet 相连。S7606 之间相连的端口均为 Trunk 端口，S7606 与 S2924G 之间相连的端口也均为 Trunk 端口。

部分 PC 的 IP 信息及所属 VLAN 如表 3-1 所示。

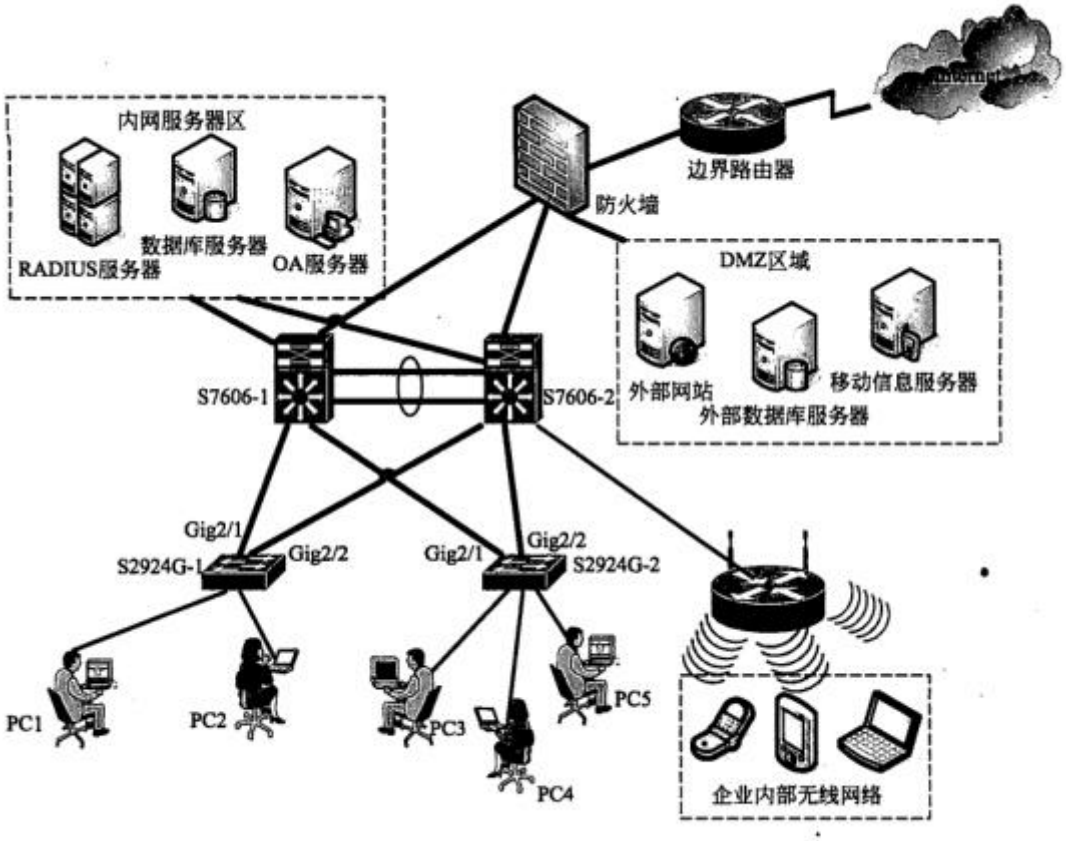


图 3-1 某企业网络拓扑结构

表 3-1 部分 PC 的 IP 信息及所属 VLAN

网络设备	IP 地址	所属 VLAN
PC1	202.10.9.10/24	VLAN 9
PC2	202.10.10.10/24	VLAN 10
PC3	202.10.11.10/24	VLAN 11
PC4	202.10.12.10/24	VLAN 12
PC5	202.10.9.15/24	VLAN 9

【问题 1】

4 台交换机都启用了 MSTP 生成树模式，其中 S7606-1 的相关配置如下：

```
S7606-1 (config)#spanning-tree mst 1 priority 4096 //缺省值是 32768
S7606-1 (config)#spanning-tree mst configuration
S7606-1 (config-mst)#instance 1 vlan 10,12
S7606-1 (config-mst)#instance 2 vlan 9,11
S7606-1 (config-mst)#name region1
S7606-1 (config-mst)#revision 1
```

S7606-2 的相关配置如下：

```
S7606-2 (config)#spanning-tree mst 2 priority 4096
S7606-2 (config)#spanning-tree mst configuration
S7606-2 (config-mst)#instance 1 vlan 10,12
S7606-2 (config-mst)#instance 2 vlan 9,11
```

两台 S2924G 交换机也配置了相同的实例、域名称和版本修订号。

(1)请问 instance2 的生成树的根交换机是哪一台？为什么？

(2)就 instance1 而言，交换机 S2924G-1 的根端口是哪个端口？为什么？

(3)请指出 PC1 发给 PC5 的数据包经过的设备路径。

(1)instance2 的生成树的根交换机是 S7606-2，因为其优先级的值较小，优先成为该实例的根交换机。(2 分)

(2)对 instance1 而言，交换机 S2924G-1 的根端口是 Gig2/1 端口，因为 instance1 的生成树的根交换机是 S7606-1，交换机 S2924G-1 离根桥最近的端口为根端口。(2 分)

(3)PCI→S2924G-1→S7606-2→S2924G-2→PC5(2 分)

(4)PVST/PVST+是 Cisco 公司提出的生成树协议，核心思想是为每个 VLAN 都计算一个生成树，这样可以在具有链路冗余保护的情况下，实现第二层的负载ˆ衡。PVST/PVST+存在的问题是：由于每个 VLAN 都需要维护一个生成树，BPDU 的通信量较大：当 VLAN 个数较多的时候，维护多棵生成树的计算量和资源占用量将急剧增长：属于私有协议。(3 分)

本题主要考查 STP、MSTP 和 PVST/PVST+相关知识点。MSTP (multiple spanning tree protocol，多生成树协议)将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。MSTP 兼容 STP 和 RSTP，并且可以弥补 STP 和 RSTP 的缺陷。它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

MST 域(multiple spanning treeregions，多生成树域)是由交换网络中的多台交换机

以及它们之间的网段构成。这些交换机都启动了 MSTP、具有相同的域名、相同的 VLAN 到生成树映射配置和相同的 MSTP 修订级别配置，并且物理上有链路连通。

一个交换网络可以存在多个 MST 域。用户可以通过 MSTP 配置命令把多台交换机划分在同一个 MST 域内。域内所有交换机都有相同的 MST 域配置：域名相同 regionl VLAN 与生成树的映射关系相同(VLAN 10 和 VLAN 12 映射到生成树实例 1，VLAN 9 和 VLAN 11 映射到生成树实例 2)。

在本问题中，配置 S7606-1 交换机在 instance 1 中的优先级为 4096，缺省是 32768，值越小越优先成为该 instance 中的根交换机。同理，instance 2 的生成树的根交换机是 S7606-2，因为其优先级的值较小，优先成为该实例的根交换机。

对 instance1 而言，交换机 S2924G-1 的根端口是 Gig2/1 端口，因为 instance1 的生成树的根交换机是 S7606-1，交换机 S2924G-1 离根桥最近的端口为根端口。

PC1 和 PC5 都属于 VLAN9，同时 VLAN9 被映射到实例 2，由于实例 2 生成树的根交换机是 S7606-2，根据生成树算法，对实例 2 而言，S2924G-1 的根端口是 Gig2/2，S2924G-2 的根端口也是 Gig2/2。因此 PC1 到 PC5 的传输路径是：

PCI→S2924G-1(Gig2/2)→S7606-2→S2924G-2(Gig2/2)→PC5

MSTP 与 PVST/PVST+之间的区别：

每个 VLAN 都生成一棵树是一种比较直接而且最简单的解决方法。它能够保证每一个 VLAN 都不存在环路。但是由于种种原因，以这种方式工作的生成树协议并没有形成标准，而是各个厂商各有一套，尤其是以 Cisco 的 VLAN 生成树 PVST(Per VLAN Spanning Tree)为代表。为了携带更多 A 信息，PVST BPDU 的格式和 STP/RSTP BPDU 格式已经不一样，发送的目的地址也改成了 Cisco 保留地址 01-00-0C-CC-CC-CD，而且在 VLAN Trunk 的情况下 PVST BPDU 被打上;T802.1Q VLAN 标签。所以，PVST 协议并不兼容 STP/RSTP 协议。

Cisco 很快又推出了经过改进的 PVST+协议，并成为其交换机产品的默认生成树协议。经过改进的 PVST+协议在 VLAN 1 上运行的是普通 STP 协议，在其他 VLAN 上运行 PVST 协议。PVST+协议可以与 STP/RSTP 互通，在 VLAN 1 上生成树状态按照 STP 协议计算。在其他 VLAN 上，普通交换机只会把 PVST BPDU 当作多播报文按照 VLAN 号进行转发。但这并不影响环路的消除，只是 VLAN 1 和其他 VLAN 的根桥状态可能不一致。由于每个 VLAN 都有一棵独立的生成树，单生成树的种种缺陷都被克服了。同时，PVST 带来了新的好处，那就是二层负载均衡。

PVST/PVST+协议也有它的明显不足：(1)由于每个 VLAN 都需要生成一棵树，PVSTBPDU

的通信量将正比于 Trunk 的 VLAN 个数。(2)当 VLAN 个数比较多时，维护多棵生成树的计算量和资源占用量将急剧增长。特别是当 Trunk 了很多 VLAN 的接口状态发生变化的时候，所有生成树的状态都要重新计算，CPU 将不堪重负。(3)由于协议的私有性，PVST/PVST+不能像 STP/RSTP一样得到广泛的支持，不同厂家的设备并不能在这种模式下直接互通。

多生成树协议 MSTP(Multiple Spanning Tree Protocol)是 IEEE802.1s 中定义的一种新型多实例化生成树协议。MSTP 协议的精妙之处在于把支持 MSTP 的交换机和不支持 MSTP 的交换机划分成不同的区域，分别称作 MST 域和 SST 域。在 MST 域内部运行多实例化的生成树，在 MST 域的边缘运行 RSTP 兼容的内部生成树 IST(lntemal Spanning Tree)。

MSTP 定义了“实例”(Instance)和域的概念。简单地说，STP/RSTP 是基于端口的，PVST/PVST+是基于 VLAN 的，而 MSTP 就是基于实例的。所谓实例就是多个 VLAN 的一个集合，通过将多个 VLAN 捆绑到一个实例可以节省通信开销和资源占用率。

MSTP 带来的好处是显而易见的。它既有 PVST 的 VLAN 认知能力和负载均衡能力，又拥有可以和 SST 媲美的低 CPU 占用率。

【问题 2】

在三层交换机 S7606-1 中 VLAN 10 的 IP 地址配置为 202.10.10.1/24，VLAN 11 的 IP 地址配置为 202.10.11.254/24。

在三层交换机 S7606-2 中 VLAN 10 的 IP 地址配置为 202.10.10.254/24，VLAN 11 的 IP 地址配置为 202.10.11.1/24。两台三层交换机中的 VRRP 配置如下：

```
S7606-1 (config)# interface Vlan 10
S7606-1 (config-if)# vrrp 10 ip 202.10.10.1
S7606-1 (config-if)# vrrp 10 preempt
S7606-1 (config)# interface Vlan 11
S7606-1 (config-if)# vrrp 11 ip 202.10.11.1

S7606-2 (config)# interface Vlan 10
S7606-2 (config-if)# vrrp 10 ip 202.10.10.1
S7606-2 (config)# interface Vlan 11
S7606-2 (config-if)# vrrp 11 ip 202.10.11.1
S7606-2 (config-if)# vrrp 11 preempt
```

(1)PC2 主机中设置的网关 IP 为 202.10.10.1，在网络正常运行的情况下，请按照以下格式写出 PC2 访问 Intemet 的数据转发路径。(格式：PC2→设备 1→…→Internet。不写返回路径)

(2)假设三层交换机 S7606-1 需要临时宕机 1 小时进行检修及升级操作系统。请问这 1 小时时段内 PC2 在没有修改网关 IP 地址的情况下，是否能访问 Internet?
请结合交换机 S7606-1 宕机后发生的变化说明原因。

(1)在网络正常运行的情况下，PC2 访问 Internet 的数据转发路径为：
PC2→S2924G-1→S7606-1→防火墙→边界路由器→Internet(2 分)

(2)能访问 Inteme。(2 分)

(3)虚拟路由冗余协议 VRRP 是用于实现路由器冗余的协议，对共享多存取访问介质(如以太网)上终端 IP 设备的默认网关(Default Gateway)进行冗余备份，从而在其中一台路由设备宕机时，备份路由设备及时接管转发工作，向用户提供透明的切换，提高了网络服务质量。

根据给出的配置可知，在网络正常情况下，VRRP 组 10 的主控路由器是 S7606-1，备份路由器是 S7606-2。当交换机 S7606-1 宕机后，经过主路由器失效间隔时间后，备份路由器会自动切换为主控路由器，整个过程对用户是透明的，因此客户机并不需要修改网关 IP，仍可以连接 Internet。(4 分)

本问题主要考查 VRRP 相关知识点。

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)坏掉时，本网段内的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，以及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 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。VRRP 协议使用选择策略从

路由器组中选出一台作为主控，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。当由于某种原因主控路由器发生故障时，备份路由器能在几秒钟的时延后升级为主路由器。由于此切换非常迅速而且不用改变 IP 地址和 MAC 地址，故对终端使用者系统是透明的。—

一个 VRRP 路由器有唯一的标识：VRID，范围为 0～255。该路由器对外表现为唯一的虚拟 MAC 地址，地址的格式为 00-00-5E-00-01-[VRID]。主控路由器负责对 ARP 请求用该 MAC 地址做应答。这样，无论如何切换，保证给终端设备的是唯一一致的 IP 和 MAC 地址，减少了切换对终端设备的影响。

VRRP 控制报文只有一种：VRRP 通告(advertisement)。它使用 IP 多播数据包进行封装，组地址为 224.0.0.18，发布范围只限于同一局域网内。这保证了 VRID 在不同网络中可以重复使用。为了减少网络带宽消耗，只有主控路由器才可以周期性地发送 VRRP 通告报文。备份路由器在连续三个通告间隔内收不到 VRRP 或收到优先级为 0 的通告后启动新的一轮 VRRP 选举。

在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中优先级范围是 0～255。若 VRRP 路由器的 IP 地址和虚拟路由器的接口 IP 地址相同，则称该虚拟路由器作 VRRP 组中的 IP 地址所有者；IP 地址所有者自动具有最高优先级：255。优先级 0—般用在 IP 地址所有者主动放弃主控者角色时使用。可配置的优先级范围为 1～254。优先级的配置原则可以依据链路的速度和成本、路由器性能和可靠性以及其他管理策略设定。主控路由器的选举中，高优先级的虚拟路由器获胜，因此，如果在 VRRP 组中有 IP 地址所有者，则它总是作为主控路由的角色出现。对于相同优先级的候选路由器，按照 IP 地址大小顺序选举。VRRP 还提供了优先级抢占策略，如果配置了该策略，高优先级的备份路由器便会剥夺当前低优先级的主控路由器而成为新的主控路由器。

为了保证 VRRP 协议的安全性，提供了两种安全认证措施：明文认证和 IP 头认证。明文认证方式要求：在加入一个 VRRP 路由器组时，必须同时提供相同的 VRID 和明文密码。适合于避免在局域网内的配置错误，但不能防止通过网络监听方式获得密码。IP 头认证的方式提供了更高的安全性，能够防止报文重放和修改等攻击。

在本小题中，在两台 S7606 中都配置了两个虚拟备份组，虚拟备份组 10 的 IP 地址为 202.10.10.1/24;虚拟备份组 11 的 IP 地址为 202.10.11.1/24。虚拟备份组 10 为 VLAN 10 中的主机提供了网关冗余，虚拟备份组 11 为 VLAN 11 中的主机提供了网关冗余。

由于 VRRP 路由器 S7606-1 的 IP 地址和虚拟备份组 10 的 IP 地址相同,因此其具有最高优先

级，成为虚拟备份组 10 的主控路由器，S7606-1 为虚拟组 10 的备份路由器。

在网络正常运行的情况下，主机 PC2 访问 Intemet 的数据转发路径为：

PC2→S2924G-1→S7606-1→防火墙→边界路由器→Intemet。

当路由器 S7606-1 宕机后，PC2 不用修改网关 IP 地址，就可以访问 Internet。因为当虚拟备份组 10 的备份路由器 S7606-2 在数秒之内没有收到主控路由器的通告，会认为主控路由器失效，就会自动启动切换，成为主控路由器，响应对虚拟 IP 地址的 ARP 请求，并且响应的是虚拟 MAC 地址，而不是接口的真实 MAC 地址。同时负责转发目的 MAC 地址为虚拟 MAC 地址的 IP 报文，这样就保证了对客户透明的网关切换。

【问题 3】

企业内部架设有无线局域网，并采用了 802.1X 认证，用户名和密码存放在 Radius 服务器的数据库中。无线路由器 Wirelessrouterl 支持 802.1x 协议，请回答以下问题：

(1)在图 3-2 所示的认证过程中，客户端向无线路由器发送的是什么帧？无线路由器向 Radius 服务器发送的是什么报文？

(2)在无线路由器中需要配置哪些与 Radius 服务器相关的信息？

(3)如果无线路由器不支持 802.1X 认证，为满足无线用户必须经过认证才能上网的需求，能否在上层交换机中启用 802.1X，并将端口设置为启用 dot1 x 认证？请简要说明理由。

图 3-2 802.1x 认证示意图

(1)客户端向无线路由器发送的是 EAPoL(Extensible Authentication Protocol over LAN)帧；无线路由器向 RADIUS 服务器发送的是 EAP over RADIUS 报文，因为认证系统将 EAP 帧封装到 RADIUS 报文中发送给认证服务器。(2 分)

(2)在无线路由器中需要配置的 RADIUS Server 信息有：IP 地址、认证和授权端口(只写端口也可以)、与 RADIUS 服务器一致的密钥。(3 分)

(3)如果无线路由器不支持 802.1X 认证，可以在上层交换机中启用 802.1X，并将端口设置为启用 dot1x 认证。但注意上层交换机下联无线路由器的 802.1X 端口认证模式应设置为 mac-based。这样接入物理端口的所有主机都需要进行认证才能访问网络资源。当某用户下线时，将不影响其他用户的认证状态，其他用户还可以继续访问网络。(3 分)

IEEE 802.1X 是根据用户 ID 或设备，对网络客户端(或端口)进行鉴权的标准。该流程被称为“端口级别的鉴权”。它采用 RADIUS(远程认证拨号用户服务)方法，并将其划分为三个不同的小组：请求方、认证方和授权服务器。802.1x 标准应用于试图连接到端口或其他设备(如 Cisco Catalyst 交换机或 Cisco Aironet 系列接入点)(认证方)的终端设备和用户(请求方)。认证和授权都通过鉴权服务器(如 CiscoSecureACS)后端通信实现。IEEE 802.1x 提供自动用户身份识别，集中进行鉴权、密钥管理和 LAN 连接配置。整个 802.1x 的实现设计三个部分：请求者系统、认证系统和认证服务器系统。

请求者是位于局域网链路一端的实体，由连接到该链路另一端的认证系统对其进行认证。请求者通常是支持 802.1x 认证的用户终端设备，用户通过启动客户端软件发起 802.1X 认证。认证系统对连接到链路对端的认证请求者进行认证。认证系统通常为支持 802.1x 协议的网络设备，它为请求者提供服务端口，该端口可以是物理端口，也可以是逻辑端口，一般在用户接入设备(如 LANSwitch 和 AP)上实现 802.1x 认证。请求者和认证系统之间运行 802.1x.定义的 EAPoL(Extensible Authentication Protocol over LAN)协议。当认证系统工作于中继方式时，认证系统与认证服务器之间运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其他高层次协议中(如 RADIUS)，以便穿越复杂的网络到达认证服务器；当认证系统工作于终结方式时，认证系统终结 EAPoL 消息，并转换为其他认证协议(如 RADIUS)，传递用户认证信息给认证服务器系统。认证系统每个物理端口内部包含有受控端口和非受控端口。非受控端口始终处于双向连通状态，主要用来传递 EAPoL 协议帧，可随时保证接收认证请求者发出的 EAPoL 认证报文；受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。

在无线路由器中需要配置的 RadiusServer 信息有：IP 地址、认证和授权端口(只写端口也可以)、与 RADIUS 服务器一致的密钥。

RADIUS 是 Remote Authentication Dial-In User Service(远程认证拨号用户服务)的简称，作为一种分布式的客户机/服务器系统，能提供 AAA 功能。RADIUS 技术可以保护网络

不受未授权访问的干扰，常被用在既要求较高安全性、又要求维持远程用户访问的各种网络环境中(如用来管理使用串口和调制解调器的大量分散拨号用户)。

RADIUS 服务包括三个组成部分：

(1)协议：rfc2865、2866 协议基于 udp/ip 层定义了 RADIUS 帧格式及消息传输机制，并定义了 1812 作为认证端口，1813 作为计费端口。(2)服务器：RADIUS 服务器运行在中心计算机或工作站上，包含了相关的用户认证和网络服务访问信息。(3)客户端：位于拨号访问服务器 NAS(Network Access Server)侧，可以遍布整个网络。

RADIUS 基于客户/服务器模型，NAS(如路由器)作为 RADIUS 客户端，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理(如接入/挂断用户)。RADIUS 服务器负责接收用户连接请求，认证用户，然后给 NASS 回所有需要的信息。RADIUS 服务器对用户的认证过程通常需要利用 NAS 等设备的代理认证功能,RADIUS 客户端和 RADIUS 服务器之间通过共享密钥认证相互间交互的消息，用户密码采用密文方式在网络上传输，增强了安全性。RADIU 民协议合并了认证和授权过程，即响应报文中携带了授权信息。

题中无线路由器即为 NAS，要使得它能与 RADIUS 服务器正常通信，根据上述原理，在无线路由器中需要配置 RADIUS 服务器的 IP 地址、认证和授权端口、与 RADIUS 服务器一致的密钥。

如果无线路由器不支持 802.1x 认证，只要在上层交换机中启用 802.1x，并将端口设置为启用 dot1 x 认证，就可以达到通过 RADIUS 服务器进行验证的功能。这种方式有两种认证模式：port-based 和 mac-based。port-based 模式下，只要物理端口下的第一个用户认证成功后，其他接入该端口的用户无需认证就可以访问网络资源，当第一个用户下线后，端口被“关闭”，其他用户也会被阻止访问网络。而在 mac-based 模式下，接入物理端口的所有主机都需要进行认证才能访问网络资源，当某用户下线时，将不影响其他用户的认证状态，其他用户还可以继续访问网络。如果端口通过交换机接入了多台主机，那么为了使每台主机都要进行认证，应使用此认证模式。

试题一 论校园网/企业网的网络规划与设计

校园网(或企业网)是计算机网络的一大分支，有着非常广泛的应用及代表性。对于校园网/企业网，完备的应用是关键，而稳定可靠的网络是基础，完善的安全和管理手段是保障。由于学校/企业的类型和规模的不同，校园网/企业网的规划设计有着多种解决方案。校园网的规划、设计、硬件建设、软件建设以及网络的使用、扩充等都要从全局、长远的角度出发，充分考虑网络的安全性、易用性、可靠性和经济性等。

请围绕“论校园网/企业网的网络规划与设计”论题，依次对以下三个方面进行论述。

1.概要叙述你参与设计实施的网络项目以及你所担任的主要工作。

2.具体讨论在校园网/企业网网络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的校园网/企业网网络的实际运行效果。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

一、论文论述的是校园网/企业网网络，要体现出校园网/企业网的应用背景，例如校园网中的教学、科研、资源共享等，企业网中的生产、销售、库存等应用。

二、叙述自己参与设计和实施的校园网/企业网网络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分量。

三、能够全面和准确地描述该校园网/企业网网络的应用环境和需求，深入地阐述采用了哪些技术和方法，这些技术和方法要针对校园网/企业网网络的特点，具有一定的广度和深度。

四、对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 论网络规划与设计中新技术的使用

随着计算机技术和通信技术的迅猛发展，计算机网络技术的发展也可用日新月异来形容。在计算机网络的交换技术、网络安全技术、光通信技术、无线通信技术、网络存储技术等诸多方面不断地涌现出各种新技术。在网络规划和设计中，如何根据项目的现状和实际需求，积极地引进和使用新技术，是网络规划设计师的职责。

请围绕“网络规划中新技术的使用”论题，依次对以下三个方面进行论述。

1.概要叙述你参与设计和实施的网络应用项目以及你所担任的主要工作。

2.具体阐述你在网络规划与设计中采用了哪些新技术和新方法，使用这些新技术和新方法的应用背景、需求和目的是什么？

3.分析你使用上述新技术、新方法的效果如何，以及相关的改进措施。

写作要点

一、论文论述着眼点是网络技术，且是新技术，所论述的技术过于陈旧就不符合要求。网络新技术可以涉及：光通信技术、无线通信技术、网络存储技术、安全技术等方面。理论上比较成熟而在工程上没有大规模普及应用的技术也可算新技术，例如 IPv6 技术等。

二、叙述自己参与设计和实施的网络应用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分量。

三、能够全面和准确地描述采用新技术和新方法的应用背景、需求和目的，深入地阐述采用了哪些新技术和新方法，这些技术和方法要符合应用背景和需求，具有一定的广度和深度，而不是堆砌技术。

四、对需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。