

全国计算机技术与软件专业技术资格（水平）考试

2009 年下半年 网络工程师 试题分析

- 本资料仅用于考生学习与讨论，禁止任何形式的商业用途。
- 本资料涉及试题分析仅供学习参考，并非官方公布数据，特此说明。
- 欢迎选择电脑报数位学院！<http://www.cpcwedu.com>

TEL: 023-63658811 QQ: 20797717、20797727

上午试题分析

- (1) B 试题解析：PC 不可以存储算术/逻辑运算结果。
- (2) A 试题解析：CISC 的指令系统对应的控制信号复杂，大多采用微程序控制器方式。
- (3) A 试题解析：海明码使用多组数位进行异或运算来检错和纠错。不过，异或也可以当做是奇偶计算，因此 A 可以算是正确的。
- B 的错误在于码距不能等于 1。
- C 的错误在于 CRC 不具有纠错能力。

取两个相近的码字，如 0 和 1，再随使用个生成多项式（如 101）进行计算，可以看出即使要传输的码字的码距为 1，但整个编码（原数据+CRC 校验码）的码距必定大于 1。如果码距可以等于 1 的话，那么就意味着 CRC 编码可能无法检查出一位的错误。因此 D 也是错误的。

不过，D 的表达存在不严谨的地方。如果将题目中的“循环冗余校验码”定为整个编码（原数据+CRC 校验码），则 D 是错误的。如果将题目中的“循环冗余校验码”定为 CRC 校验码，则 D 是正确的。

(4) B 试题解析: A、C、D 都明显错误。

(5) D 试题解析: Jackson 是面向数据结构的设计方法。

(6) A 试题解析: 常识。

(7) C 试题解析: 在软件生命周期中的任何一个阶段, 只要软件发生了改变, 就可能给该软件带来问题。软件的改变可能是源于发现了错误并做了修改, 也有可能是因为在集成或维护阶段加入了新的模块。当软件中所含错误被发现时, 如果错误跟踪与管理系统不够完善, 就可能会遗漏对这些错误的修改; 而开发者对错误理解的不够透彻, 也可能导致所做的修改只修正了错误的外在表现, 而没有修复错误本身, 从而造成修改失败; 修改还有可能产生副作用从而导致软件未被修改的部分产生新的问题, 使本来工作正常的功能产生错误。同样, 在有新代码加入软件的时候, 除了新加入的代码中有可能含有错误外, 新代码还有可能对原有的代码带来影响。因此, 每当软件发生变化时, 我们就必须重新测试现有的功能, 以便确定修改是否达到了预期的目的, 检查修改是否损害了原有的正常功能。同时, 还需要补充新的测试用例来测试新的或被修改了的功能。为了验证修改的正确性及其影响就需要进行回归测试。

(8) B (9) D 试题解析: 常识。

(10) A 试题解析: 许可贸易实际上是一种许可方用授权的形式向被许可方转让技术使用权同时也让度一定市场的贸易行为。根据其授权程度大小, 许可贸易可分为如下五种形式:

(1) 独占许可。它是指在合同规定的期限和地域内, 被许可方对转让的技术享有独占的使用权, 即许可方自己和任何第三方都不得使用该项技术和销售该技术项下的产品。所以这种许可的技术使用费是最高的。

(2) 排他许可, 又称独家许可; 它是指在合同规定的期限和地域内, 被许可方和许可方自己都可使用该许可项下的技术和销售该技术项下的产品, 但许可方不得再将该项技术转让给第三方。排他许可是仅排除第三方面不排除许可方。

(3) 普通许可。它是指在合同规定的期限和地域内, 除被许可方该允许使用转让的技术和许可方仍保留对该项技术的使用权之外, 许可方还有权再向第三方转让该项技术。普通许可是许可方授予被许可方权限最小的一种授权, 其技术使用费也是最低的。

(4) 可转让许可, 又称分许可。它是指被许可方经许可方允许, 在合同规定的地域内, 将其被许可所获得的技术使用权全部或部分地转售给第三方。通常只有独占许可或排他许可的被许可方才获得这种可转让许可的授权。

(5) 互换许可, 又称交叉许可。它是指交易双方或各方以其所拥有的知识产权或专有技术, 按各方都同意的条件互惠交换技术的使用权, 供对方使用。这种许可多适用于原发明的专利权人与派生发明的专利权人之间。

(11) D (12) C 试题解析: E1 的一个时分复用帧的传送时间为 $125\ \mu\text{s}$, 即每秒 8000 次。

一个帧的传送时间被划分为 32 相等的子信道, 信道的编号为 CH0-CH31。其中信道 CH0 用作帧同步用, 信道 CH16 用来传送信令, 剩下 CH1-CH15 和 CH17-CH31 共 30 个信道可用于用户数据传输。

(13) A (14) C 试题解析: 4B / 5B 编码是将欲发送的数据流每 4bit 作为一个组, 然后按照 4B / 5B 编码规则将其转换成相应 5bit 码。5bit 码共有 32 种组合, 但只采用其中的 16 种作为数据码对应 4bit 码; 其它的 16 种或者未用, 或者作为控制码用于表示帧的开始和结束、光纤线路的状态(静止、空闲、暂停)等。

4B / 5B 编码可以在 NRZ-I 编码的基础上实现, 但由于 NRZ-I 编码(非归零反相编码)没有解决传输比特 0 的同步问题, 因此, 4B / 5B 编码的设计目的是保证整个传输数据信息(不包括控制信息)的过程中, 无论是单组编码还是相邻组编码, 都不会出现超过 3 个连续“0”的情况。通过 4B / 5B 的特别编码方式, 解决传输中的同步问题。

(15) C (16) B 试题解析: 两种编码都在比特间隙的中央有跳变, 说明它们都属于双相位编码。因此(15)题答案只能在 A、C 中选择。

如果(15)题选 A, 则 x 为差分曼彻斯特编码。差分曼彻斯特编码的比特间隙中间的跳变仅用于携带同步信息, 不同比特是通过在比特间隙开始位置是否有电平跳变来表示。每比特的开始位置没有电平跳变表示比特 1, 有电平跳变表示比特 0。

如果将 x 编码当做差分曼彻斯特编码, 其数据应该是? 11010111(第一位编码由于无法预知其前状态, 因此只能用? 表示)。y 编码可能是“011101100”或“100010011”, 显然差分曼彻斯特编码和曼彻斯特编码的结果对应不上, 因此 A 是错误的。

如果(15)题选 C, 则 y 为差分曼彻斯特编码, 其数据应该是? 10011010。x 编码可能是“010011010”或“101100101”。显然第一个结果能够与差分曼彻斯特编码的结果匹配。所以可以判定该数据位为 010011010。

(17) B (18) C 试题解析: 这个信号明显是属于相位调制, 在(17)题的备选答案中, PSK 是相移键控, 满足题意。

DPSK(Differential Phase Shift Keying, 差分相移键控)波形的同一个相位并不一定代表相同的数字信号, 而前后码元的相对相位才能唯一地确定数字信息, 所以只要前后码元的相对相位关系不破坏, 就可正确恢复数字信息。这就避免了绝对 PSK 方式中的“倒 π ”现象的发生, 因此得到广泛的应用。

在数字信号中, 一个数字脉冲称为一个码元(Symbol), 一次脉冲的持续时间称为码元的宽度。码元速率(Symbol Rate)表示单位时间内信号波形的最大变换次数, 即单位时间内通过信道的码元个数。码元速率即数字信号中的波特率, 所以码元速率的单位也为 baud/s。

在这个信号中, 由于码元宽度为 2 个载波信号周期, 因此其码元速率为 1200baud/s。

(19) D (20) A 试题解析: 电信号在铜缆上的传播速度大致为光速的 $2/3$, 也就是每秒 20 万公里。

(19) 题的答案是总传输时间=传输延迟时间+数据帧的发送时间= $2000 / 200000 + 3000 / 4800 = 10\text{ms} + 625\text{ms} = 635\text{ms}$ 。

(20) 题有些含混, 毕竟信号要先发到太空的卫星上, 再转发到 2000km 外的接收站, 因此总距离不可能还是 2000km。不过题目没有提供相关数据, 因此就还是使用 2000km 当做传输距离。总传输时间=传输延迟时间+数据帧的发送时间= $2000 / 300000 + 3000 / 50000 = 6.7\text{ms} + 60\text{ms} = 66.7\text{ms}$ 。在所有备选答案中, 也就只有 A 比较相近, 那么也就只能选 A 了。至于多出来的 3.3ms, 就当是上天下地增加的传输延迟吧。

至于有人提出卫星传输的延时是 270ms, 这里要说明一下: 传输延时是与距离相关的, 距离越远则延时越大。即使是同一颗卫星, 其近地点与远地点的通信传输延迟都差别非常大。如果死记 270ms, 那就是教条主义了。

(21) B 试题解析: 选择重传 ARQ 协议必须严格控制窗口大小, 使得 $W \leq 2^{K-1}$ (K 为帧编号字段长), 否则接收方可能会把重发的帧当作新的帧, 造成协议的失败。

(22) D (23) B 试题解析: RIP 是基于 D-V 算法的路由协议, 由于 D-V 算法存在着路由收敛速度慢的问题, 因此 RIPv2 采用了触发更新等机制来加速路由计算。

RFC 1388 对 RIP 协议进行了扩充, 定义了 RIPv2。RIPv1 使用广播方式进行路由更新, RIPv2 改为组播方式进行路由更新。RIPv2 使用的组播地址是 224.0.0.9。

RIPv1 不具备身份验证功能, 这样就存在有安全漏洞。RIPv2 实现了身份验证功能, 能够通过路由更新消息中的口令来判断消息的合法性。RIPv2 支持两种类型的身份验证: 明文口令和 MD5 散列口令。明文口令安全性差, 不推荐使用。当使用 MD5 散列口令时, 发送方使用 MD5 单向散列函数将路由更新消息和口令一起计算出一个摘要值, 然后将路由更新消息和摘要值一起发送出去; 接收方收到路由更新消息后, 使用相同的方法也计算出一个摘要值, 将收到的摘要值和自己计算出来的摘要值进行对比, 如果相等, 说明双方使用了相同的 MD5 散列口令。由于 MD5 散列口令并非直接在网络上以明文形式进行传输, 因此具有较高的安全性。

使用共同口令的路由器构成了一个身份验证区域。一个网络中的路由器使用多个口令时, 就可以构成多个身份验证区域。因此, RIPv2 可以通过设置不同的身份验证口令来限制路由信息的传播。

RIPv2 的每个路由记录都携带有自己的子网掩码, 因此实现了对 CIDR (Class Inter-Domain Routing, 无类域间路由)、VLSM (Variable Length Subnetwork Mask, 可变长子网掩码) 和不连续子网的支持。但不涉及对 NAT 的支持。

水平分割方法的原理是: 路由器必须有选择地将路由表中的路由信息发送给相邻的其它路由器, 而不是发送整个路由表。具体地说, 即一条路由信息不会被发送给该信息的来源方。

(24) C (25) D 试题解析: 如果将区域看成一个节点, 则 OSPF 是以主干区域(area 0)为顶点, 其他区域为终端的星形拓扑结构。

标准区域可以接收链路更新信息和路由总结。

存根区域是不接受自治系统以外的路由信息的区域。如果需要自治系统以外的路由, 它使用默认路由 0.0.0.0。

完全存根区域不接受外部自治系统的路由以及自治系统内其他区域的路由总结, 需要发送到区域外的报文则使用默认路由 0.0.0.0。完全存根区域是 Cisco 自己定义的。

不完全存根区域类似于存根区域, 但是允许接收以 LSAType7 发送的外部路由信息, 并且要把 LSAType7 转换成 LSAType5。

(26) B 试题解析:

MPLS 提供多种协议的接口, 如 IP、ATM、帧中继、资源预留协议 (RSVP)、开放最短路径优先 (OSPF) 等。MPLS 将 IP 地址映射为简单的具有固定长度的标签, 用于不同的包转发和包交换技术。

(27) A (28) C (29) C 试题解析: 略。

(30) B (31) C (32) A 试题解析: ps 命令显示系统正在运行的进程, 参数: e 列出系统所有的进程, f 列出详细清单。

显示各列为:

- ★ UID: 运行进程的用户
- ★ PID: 进程的 ID
- ★ PPID: 父进程的 ID
- ★ C: 进程的 CPU 使用情况 (进程使用占 CPU 时间的百分比)
- ★ STIME: 开始时间
- ★ TTY: 运行此进程的终端或控制台
- ★ TIME: 消耗 CPU 的时间总量
- ★ CMD: 产生进程的命令名称

Linux 操作系统内核被加载入内存后, 开始掌握控制权。接着, 它将完成对外围设备的检测, 并加载相应的驱动程序, 如软驱、硬盘、光驱等。然后, 系统内核调度系统的第一个进程, init 进程。

作为系统的第一个进程, init 的进程 ID (PID) 为 1。它将完成系统的初始化工作, 并维护系统的各种运行级别, 包括系统的初始化、系统结束、单用户运行模式和多用户运行模式。

在 Linux 系统中, 大部分的服务进程 (daemon) 都会设置成在系统启动时自动执行。服务进程是指在系统中持续执行的进程。但是, 过多进程同时执行必然会占据更多的内存、CPU 时间等资源, 从而使系统性能下降。为了解决这个问题, Linux 系统提供了一个超级服务进程: inetd/xinetd。

inetd/xinetd 总管网络服务, 使需要的程序在适当时候执行。当客户端没有请求时, 服务进程不执行; 只有当接收到客户端的某种服务器请求时, inetd/xinetd 根据其提供的

信息去启动相应的服务进程提供服务。

inetd/xinetd 负责监听传输层协议定义的网络端口。当数据包通过网络传送到服务器时, inetd/xinetd 根据接收数据包的端口判断是哪个功能的数据包, 然后调用相应的服务进程进行处理。除 Red Hat Linux 7 使用 xinetd 来提供这个服务外, 大部分版本的 Linux 系统都使用 inetd。

(33) C 试题解析: inetd.conf 是系统超级服务进程 inetd 的配置文件。

lilo.conf 是操作系统启动程序 LILO 的配置文件。

httpd.conf 是 web 服务器 Apache 的配置文件。

resolver.conf 是 DNS 解析的配置文件。

(34) B 试题解析: 常识。

(35) D (36) A 试题解析: route add 的格式是:

```
route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
destination      mask      gateway      metric      Interface
```

(37) D 试题解析: Microsoft 管理控制台 (MMC) 集成了可以用于管理网络、计算机、服务和其他系统组件的管理工具。它不仅仅是一个网络组件。

(38) A 试题解析: RAID 0 是非容错卷, 没有磁盘损耗

(39) B 试题解析: XDSL 的标准中有。

(40) D 试题解析: 常识。

(41) C 试题解析: Kerberos 是为 TCP/IP 网络而设计的基于客户机/服务器模式的三方验证协议, 最早源于麻省理工学院 (MIT) 的雅典娜计划, 由麻省理工学院 (MIT) 开发, 首次公开的版本为 v4, 目前广泛使用的是 v5。

在 Kerberos v4 系统中, 使用时间戳用来防止重发攻击。

在 Kerberos v5 系统中, 使用 Seq 序列号用来防止重发攻击。

由于现在主流是 Kerberos v5, 因此答案选 C。如果宽松一些, 那么选 A 也应该算对。

(42) C 试题解析: Worm 代表蠕虫;

CIH 是台湾人陈盈豪编写的一种能够攻击硬件的病毒。

Trojan 代表木马, 来源于古希腊荷马史诗中木马破城的故事 (Trojan 一词的本意是特洛伊)。木马可以进行远程控制。

Melissa 是一种快速传播的能够感染那些使用 MS Word 97 和 MS Office 2000 的计算机宏病毒。

(43) A 试题解析: `ip access-group acl_id in|out` 在指定端口上启动 ACL

(44) A (45) B (46) C 试题解析: 证书的概念, 数字证书里没有私钥。

(47) B 试题解析: AH (Authentication Header, 认证头) 是 IPSec 体系结构中的一种主要协议, 它为 IP 数据报提供完整性检查与数据源认证, 并防止重发攻击。

AH 不提供数据加密服务, 加密服务由 ESP (Encapsulating Security Payload, 封装安全载荷) 提供。ESP 提供数据内容的加密, 根据用户安全要求, ESP 既可以用于加密 IP 数据报的负载内容 (如: TCP、UDP、ICMP、IGMP), 也可以用于加密整个 IP 数据报。

进行 IPSec 通讯前必须先要在通信双方建立 SA (安全关联)。IKE (Internet Key Exchange, 因特网密钥交换) 是一种混合型协议, 用于动态建立 SA, 它沿用了 ISAKMP (Internet Security Association and Key Management Protocol, Internet 安全协作和密钥管理协议) 的框架、Oakley 的模式 (Oakley 描述了一系列的密钥交换模式, 提供密钥交换和刷新功能) 以及 SKEME (Secure Key Exchange Mechanism, Internet 安全密钥交换机制) (SKEME 描述了通用密钥交换技术, 提供匿名性、防抵赖和快速刷新等功能) 的共享和密钥更新技术, 提供密码生成材料技术和协商共享策略。

TGS (Ticket Granting Server) 是 Kerberos 的票据授权服务器。

(48) D 试题解析: 常识。

(49) B (50) A 试题解析: CIDR 每次必考, 原本不必多说, 但 50 题的备选答案有些离奇。因此, 请先看看下面这张图。



由于主机位有 11 位, 因此可分配的主机地址有 $2^{11}-2=2046$ 。但是备选答案中没有 2046, 这就有些离奇了。首先, 2048 和 2056 两个答案都是可以排除的, 接下来分析 2032 和 2000 两个备选答案。

如果误以为 CIDR 中的各成员网络的主机位全“0”和全“1”地址都不可使用 (即 192.24.0.0、192.24.0.255、……、192.24.7.0、192.24.7.255), 那也只有 16 个地址而已。即便如此, 可分配的地址也有 $2^{11}-16=2032$ 个, 离答案 A 比较接近。按道理说命题老师不至于犯这种错误, 总觉得选 2032 这个答案不对劲。

至于答案 2000, 这个未免也太小了一些, 应该不是。

因此, 我怀疑这道题有可能命题错误, 命题老师可能是想问“其中有 (50) 个主机

地址”，这样就可以选答案 B（2048）了。但现在考试已经结束了，不可能再该卷子，因此只能有两个方案：

- 1、试题有错，无论考生回答哪一个都给分。
- 2、取最接近的一个答案，那么就选 A。

(51) B 试题解析：略。

(52) D 试题解析：202.16.254.0/22 是网络 202.16.252.0/22 中一个可分配主机地址。

(53) A 试题解析：略。

(54) B (55) A 试题解析：IPv6 首部的固定部分被简称为 IPv6 首部，其大小是 40 字节，而 IPv4 首部中的必要部分为 20 字节。IPv6 已经定义了以下扩展首部：

- ★逐跳选项首部 (Hop-by-Hop Options header)：定义需要逐跳处理的特殊选项；
- ★路由首部 (Routing header)：提供扩展路由，类似于 IPv4 的源路由；
- ★片段首部 (Fragment header)：包含分片和重组信息；
- ★认证首部 (Authentication header)：提供数据完整性和认证；
- ★封装安全负载首部 (Encapsulation Security Payload header)：提供秘密性；
- ★目标选项首部 (Destination Options header)：包含要在目标节点检查的可选信息。

IPv6 标准建议，当用到多个扩展首部时，IPv6 首部要按以下顺序出现：

1. IPv6 首部：必要，必须最先出现。
2. 逐跳选项首部：此首部中包含的选项要由 IPv6 目标地址字段中第一个出现的目标以及路由首部列出的后续目标加以处理。
3. 路由首部
4. 片段首部
5. 认证首部
6. 封装安全负载首部
7. 目标选项首部：所包含的选项仅由数据包的最后目标加以处理。

(56) D 试题解析：FR 的带宽控制技术是它的一大优点。在传统的通信业务中，用户预定了一条 64Kbps 的链路，那么就只能以 64Kbps 的速率传输。而在 FR 技术中，预定的是 CIR (Committed Information Rate, 约定数据速率)，即在正常状态下 Tc (Committed Time Interval, 承诺时间间隔) 内的数据速率平均值。在实际的数据传输过程中，用户能以高于 64Kbps 的速率传送数据。举例来说，一个用户预定了 CIR=64Kbps 的 FR 链路，并与 FR 业务供应商鉴定了另外两个指标：

Bc (Committed Burst, 承诺突发量)：在承诺信息速率的测量间隔内，交换机准许接收

TEL: 023-63658811

QQ: 20797717、20797727

地址：重庆市渝中区双钢路 3 号 1307 室

邮编：400013

和发送的最大数据量，以 bps 为单位。

Be (Excess Burst, 超突发量)：在承诺信息速率之外，FR 交换机试图发送的未承诺的最大额外数据量，以 bps 为单位。超量突发依赖于厂商可以提供的服务，但是一般来说它要受到本地接入环路端口速率的限制。一般来说，发送超量突发数据 (Be) 的概率要小于承诺突发数据 (Bc)。网络把超量突发数据 (Be) 看作可丢弃的数据。

当用户以等于或低于 64Kbps (CIR) 的速率传送数据时，网络一定可靠地负责传送，当用户以大于 64Kbps 的速率传送数据，且用户在 Tc 内的发送量 (突发量) 少于 Bc+Be 时，在正常情况下也能可靠地传送，但是若出现网络拥塞，则会被优先丢弃。当突发量大于 Bc+Be 时，网络将丢弃数据帧。所以 FR 用户虽然付了 64Kbps 的信息速率费 (收费以 CIR 来定)，却可以传送高于 64Kbps 速率的数据，这是 FR 吸引用户的主要原因之一。

FR 控制呼叫使用的协议是 LAPD (Link Access Protocol Channel D, D 信道链路访问协议)。LAPD 定义在 ITU Q.921 中，与 X.25 的 LAPB 基本相同。它工作在 ABM (Asynchronous Balanced Mode, 异步平衡模式) 下，为 FR 进行信令管理提供数据链路层支持。

FR 用户数据传输使用的协议是 LAPP (Link Access Procedure to Frame mode bearer service, 帧模式承载业务链路访问过程)。LAPP 定义在 ITU Q.922 中，是一种在 FR 网络中为帧方式业务提供拥塞控制性能的增强版 LAPD，其主要功能是帧同步、虚电路复用、DLCI 管理、差错检测和拥塞控制等。

FR 使用 1 号数字用户信令 (DSS1) 进行 PVC (永久虚电路) 和 SVC (交换虚电路) 管理。DSS1 定义在 ITU Q.931 / Q.933，说明了帧方式交换、PVC 控制及状态监控的信令规程。

(57) D 试题解析: Designed to make access to Simple Network Management Protocol (SNMP) MIB objects easier, a set of UNIX-like SNMP commands has been created. The Tcl shell is enabled either manually or by using a Tcl script, and the new commands can be entered to allow you to perform specified get and set actions on MIB objects. To increase usability, the new commands have names similar to those used for UNIX SNMP access.

参看:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_tcl.html#wp1051671

(58) D 试题解析: 汇聚层是楼群或小区的信息汇聚点，是连接接入层与核心层的网络设备，为接入层提供数据的汇聚、传输、管理和分发处理。汇聚层为接入层提供基于策略的连接，如地址合并、协议过滤、路由服务、认证管理等，通过网段划分 (如 VLAN) 与网络隔离可以防止某些网段的问题蔓延和影响到核心层。汇聚层同时也可以提供接入层虚拟网之间的互联，控制和限制接入层对核心层的访问，保证核心层的安全和稳定。

汇聚层设备一般采用可管理的三层交换机或堆叠式交换机以达到带宽和传输性能的要求。其设备性能较好，但价格高于接入层设备，而且对环境的要求也较高，对电磁辐射、温度、湿度和空气洁净度等都有一定的要求。汇聚层设备之间以及汇聚层设备与核心层设备之

间多采用光纤互联，以提高系统的传输性能和吞吐量。

在汇聚层实现安全控制和身份认证时，通常采用的是集中式的管理模式。当网络规模较大时，可以设计综合安全管理策略，例如在接入层实现身份认证和 MAC 地址绑定，在汇聚层实现流量控制和访问权限约束。

实际上，组播管理也可以在汇聚层完成。无论是从分层的思想还是实际的工程来说，都没有什么绝对的不可的限制。做什么或不做什么，只是利弊问题。

但这样一来，这道题目就没有可选的答案了。犹豫了半天，最后选了 D，尽管这样对 D 来说有些冤枉。

(59) C 试题解析：常识。

(60) C 试题解析：IEEE 802.1q 标准为标识带有 VLAN 成员信息的以太帧建立了一种标准方法。IEEE 802.1q 标准定义了 VLAN 网桥操作，从而允许在桥接局域网结构中实现定义、运行以及管理 VLAN 拓扑结构等操作。IEEE 802.1q 标准主要用来解决如何将大型网络划分为多个小网络，以使广播和组播流量不会占据更多带宽。此外 IEEE 802.1q 标准还提供更高的网络段间安全性。

(61) D 试题解析：按总线争用协议来分类，CSMA 有三种类型：

1) 非坚持 CSMA。一个站点在发送数据帧之前，先要对媒体进行检测。如果没有其它站点在发送数据，则该站点开始发送数据。如果媒体被占用，则该站点不会持续监听媒体，而等待一个随机的延迟时间之后再监听。采用随机的监听延迟时间可以减少冲突的可能性，但其缺点也是很明显的：即使有多个站点有数据要发送，因为此时所有站点可能都在等待各自的随机延迟时间，而媒体仍然可能处于空闲状态，这样就使得媒体的利用率较为低下。

2) 1-坚持 CSMA。当一个站点要发送数据帧时，它就监听媒体，判断当前时刻是否有其他站点正在传输数据。如果媒体忙的话，该站点等待直至媒体空闲。一旦该站点检测到媒体空闲，它就立即发送数据帧。如果产生冲突，则等待一个随机时间再监听。之所以叫“1-坚持”，是因为当一个站点发现媒体空闲的时候，它传输数据帧的概率是 1。1-坚持 CSMA 的优点是：只要媒体空闲，站点就立即发送；它的缺点在于：假如有两个或两个以上的站点有数据要发送，冲突就不可避免。

3) P-坚持 CSMA。P-坚持 CSMA 是非坚持 CSMA 和 1-坚持 CSMA 的折中。P-坚持 CSMA 应用于划分时槽的媒体，其工作过程如下：当一个站点要发送数据帧的时候，它先检测媒体。若媒体空闲，则该站点按照概率 P 的可能性发送数据，而有 1-P 的概率会把要发送数据帧的任务延迟到下一个时槽。按照这样的规则，若下一个时槽也是空闲的，则站点同样有 P 的概率发送数据帧。

(62) B 试题解析: 运行 nslookup, 执行 help。解释 set type=X 的作用为“ set query type(ex. A, AAAA, A+AAAA, ANY, CNAME, MX, NS, PTR, SOA, SRV)” 根据这个解析, 应该选 B。

(63) B 试题解析: s 是 static 的缩写。

(64) D 试题解析: DAS (Direct Attached Storage, 直接连接存储) 将磁盘阵列、磁带库等数据存储设备通过扩展接口 (通常是 SCSI 接口) 直接连接到服务器或客户端。

NAS (Network Attached Storage, 网络连接存储) 与 DAS 不同, 它的存储设备不是直接连接到服务器, 而是直接连接到网络, 通过标准的网络拓扑结构连接到服务器。

SAN (Storage Area Network, 存储区域网络) 是一种通过专用传输通道 (光纤通道或 IP 网络) 连接存储设备和相关服务器的存储结构。

(65) C 试题解析: CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, 载波侦听多路访问/避免冲突) 是 IEEE 802.11 无线局域网的 MAC 子层协议, 主要用于解决无线局域网的信道共享访问问题。而在传统以太网中, MAC 子层采用 CSMA/CD (Carrier Sense Multiple Access with Collision Detection, 带有冲突检测的载波侦听多路访问) 协议。这两种协议都针对网络中共享信道如何分配的问题, 但它们的工作原理却有所不同。最明显的区别是: CSMA/CA 是在冲突发生前进行冲突处理而 CSMA/CD 是在冲突发生后进行冲突处理。导致这种不同的根本原因是无线局域网所采用的传输媒介和传统局域网所采用的传输媒介有着本质的区别。也正是由于这种区别, 导致无线局域网存在新的问题: 隐藏站问题和暴露站问题。这些问题都属于隐蔽终端问题。

(66) A 试题解析: 常识。

(67) A 试题解析: 工作区子系统指信息插座与数据终端之间的连接设置系统, 由从信息插座延伸至数据终端设备的连接线缆和适配器组成。它一般使用软线 (Patch Cable) 材料 (例如 UTP/STP) 实现终端设备与信息插座之间的连接。工作区的跳线 (Patch Cord)、连接设备的跳线、交叉连接 (Cross-Connection) 线的总长度一般不超过 10 米。其中交叉连接线或跳线的长度不应超过 5 米。

(68) D 试题解析: 常识。

(69) B 试题解析: 核心层是各区域网络中所有通信流量的最终汇集点和承受者, 用于实现骨干网络数据的优化传输, 其主要特征是冗余设计、负载均衡、高带宽和高吞吐率。由于核心层的目标是快速传递分组, 因此不宜集成控制功能和分组处理功能, 而且传输带宽必须是千兆或万兆级的。

核心层作为网络骨干和核心, 其设备多由核心路由器、多层交换机和服务器群组成, 具备高性能、高扩展性、高可靠性, 以及强有力的网络控制能力和管理特性。各设备之间通常采用光纤进行点对点连接, 并设计冗余线路, 以提高传输速率和可靠性。

(70) A 试题解析: 常识。

(71) B (72) D (73) B (74) C (75) A

下午试题参考答案

试题一 (共 15 分)

(1) 接入 (2) PoE

试题解析: 由于图上标有“核心交换机”和“汇聚交换机”字样, 因此 (1) 填写“接入”比较合适。

以太网供电 PoE (Power Over Ethernet) 以太网供电这项创新的技术, 指的是现有的以太网 CAT-5 布线基础架构在不用作任何改动的情况下就能保证在为如 IP 电话机、无线局域网接入点 AP、安全网络摄像机以及其他一些基于 IP 的终端传输数据信号的同时, 还能为此类设备提供直流供电的能力。PoE 技术用一条通用以太网电缆同时传输以太网信号和直流电源, 将电源和数据集成在同一有线系统当中, 在确保现有结构化布线安全的同时保证了现有网络的正常运作。

(3) 11 (4) 54 (5) D (6) C (7) A (8) E

试题解析: IEEE 802.11n 标准的核心是 MIMO (multiple-input multiple-output, 多入多出) 和 OFDM 技术, 最大传输速率可达 600Mbps, 同时采用软件的无线电技术, 可以向前向后兼容。

(9) SSID (10) MAC (11) WEP (12) WPA-PSK/WPA2-PSK (13) A

试题解析: 从目前的应用来说, 个人用户常用 WPA-PSK (pre-shared key, 预共享密钥) 认证, 而企业则一般使用 WPA-EAP (Extensible Authentication Protocol, 扩展认证协议) 认证。这是因为企业可以部署 Radius 服务器提供认证服务, 所以可以使用 EAP/802.1x 认证协议。而个人用户使用电脑数量较少, 使用 WPA-PSK 进行认证即可达到需求。

WAP2 使用了更强壮的加密算法 AES, 需要专门的硬件支持, 目前大部分的 Wi-fi 产品都支持 AES 加密。

试题二 (共 15 分)

【问题 1】 (4 分) (1) abc.edu (2) www

【问题 2】 (3 分) (3) 通过 IP 地址查询域名 (4) 210.43.16 (5) www.abc.edu

【问题 3】 (3 分) 选中“启用转发器”，在“IP 地址”输入框中输入 DNS 服务器 2 的 IP 地址，点击“添加”按钮，然后点击“确定”按钮。

【问题 4】 (2 分) (6) A

【问题 5】 (3 分) PC5 的网关设置错误。重新设置 PC5 的网关，将其改为 192.168.0.3 即可。

试题三 (共 15 分)

【问题 1】 (1 分) A 或 /etc/dhcpd.conf

【问题 2】 (4 分) (2) A 或 service dhcpd start (3) C 或 service dhcpd stop

【问题 3】 (10 分) (4) 52:54:AB:34:5B:09 (5) 192.168.1.100 (6) 255.255.255.0
(7) 192.168.1.254 (8) 192.168.1.3

试题四 (共 15 分)

【问题 1】 (4 分) (1) 添加可监听的 FTP 服务端口 21 (2) 定义外部默认路由 61.144.51.45，跳数为 1

【问题 2】 (6 分) (3) 192.168.0.1 (4) 255.255.255.248 (5) eth2 (6) 10.10.0.1

【问题 3】 (2 分) (7) 61.144.51.46

【问题 4】 (3 分) 说明:

static 命令的格式是: static(nameif, outside) ip-outside, ip-nameif

第(10)空要填写一个主机地址,这里填写的是DMZ内的那个主机的IP地址,而不是对外的那个地址。以免出现修改NAT配置后,开放的内网主机服务的命令也要跟随改动。

答案:

(8) 61.144.51.43 (9) 10.10.0.100 (10) 10.10.0.100

试题五(共15分)

【问题1】(4分)说明:

"access-list 101 permit ip (3) 0.0.0.255 (4) 0.0.0.255"的意思是“从本地站点(3)发出的和来自远点站点(4)的数据将得到保护。”

答案:

- (1) policy
- (2) 验证方法为使用预共享密钥
- (3) 10.10.20.0
- (4) 10.10.10.0

【问题2】(4分) (5) 10.10.20.0 (6) 192.168.1.1

【问题3】(空(9)1分,其他2分,共7分)

- (7) 378
- (8) 192.168.1.1
- (9) 设置IPSec变换集testvpn, AH鉴别采用ah-md5-hmac, ESP加密采用esp-des, ESP认证采用esp-md5-hmac。
- (10) testvpn